AV-Comparatives

Mobile Security Review

Sprache: Deutsch

September 2014
Letzte Überarbeitung: 29. September 2014

www.av-comparatives.org

Inhalt

Einleitung 3
Kurzübersicht 6
Getestete Produkte 8
Batterieverbrauch 9
Schutz vor Android-Schädlingen 11
AVC UnDroid Analyser 11
Android Device Manager 13
AhnLab V3 Mobile 15
avast! Mobile Security 19
Avira Antivirus Security 24
Baidu Mobile Security 28
Bitdefender Mobile Security 32
CheetahMobile Clean Master 36
CheetahMobile CM Security 40
ESET Mobile Security 44
F-Secure Mobile Security 48
G Data Internet Security 52
Ikarus mobile.security 57
Kaspersky Internet Security 60
Kingsoft Mobile Security 64
McAfee Mobile Security 67
Qihoo 360 AntiVirus 72
Quick Heal Total Security 75
Sophos Security and Antivirus 80
Tencent Mobile Manager 84
Trend Micro Mobile Security 88
Webroot SecureAnywhere Mobile Complete . 92
Fazit 96
Appendix - Berechtigungen 97
Appendix – Featurelist 98
Copyright and Disclaimer 99

Einleitung

Smartphones stellen die Zukunft der modernen Kommunikation dar. Im Jahr 2013 wurden weltweit mehr als 1 Milliarde Smartphones verkauft, was einen weiteren Meilenstein in dem unaufhaltbaren Vormarsch der Smartphones darstellt[1]. Eine von Facebook veröffentlichte Studie verdeutlicht den Stellenwert von Smartphones in unserem Leben. So benutzen etwa 80% das Smartphone innerhalb der ersten 15 Minuten nach dem Aufwachen[2].

Dabei treten die klassischen Funktionen eines Telefons immer mehr in den Hintergrund. Durch die guten Kameras muss das Smartphone immer häufiger als Fotoapparat dienen. Neben den Fotos vertrauen die Benutzer durch Dienste wie Facebook, WhatsApp und Email ihrem Smartphone praktisch ihr ganzes Leben an. Dies bringt einige Risiken mit sich, denn mit diesen Eigenschaften wird das Smartphone auch für Kriminelle interessant, die versuchen, das Handy zu infizieren oder sensible Daten auszuspionieren. Gefährlich sind auch Attacken auf persönliche Daten oder Phishing-Angriffe.

Der Einsatz eines PCs oder Laptops ohne Security-Software ist inzwischen undenkbar. Bei Mobiltelefonen ist dieses Verantwortungsbewusstsein bei vielen der Nutzer leider noch nicht angekommen. Dabei enthalten sie oft wichtige persönliche Daten, private Fotos, Internetbanking Informationen oder sogar Firmendaten.

Da moderne Smartphones oft teuer sind, werden sie auch immer öfters das Ziel von Dieben. Hochpreisige Smartphones lassen sich durchaus für mehrere hundert Euro verkaufen. Da Diebstähle an sich nicht zu verhindern sind, muss der Anreiz eines Diebstahles wegfallen. Deshalb verfügen viele der heutigen Sicherheitsprodukte neben dem klassischen Antivirenschutz über ausgereifte Diebstahlschutzfunktionen, welche einen Diebstahl für Diebe weniger attraktiv machen – wie etwa dem Sperren des Geräts, oder beim Wiederfinden des Geräts helfen sollen.

Auch in diesem Jahr haben wir Sicherheitsprodukte für Mobiltelefone unter Google Android getestet. In unserem Bericht finden Sie Details zu den Produkten führender Anbieter, die sich bereit erklärt haben ihr Produkt unserer Überprüfung zu stellen. Der Test wurde im Juli und August 2014 unter Android 4.4.2 auf einem LG Nexus 5 durchgeführt. Bei Fehlverhalten oder Problemen bei gewissen Funktionen haben wir diese auf einem alternativen Smartphone, einem Samsung Galaxy S3 Mini mit Android Version 4.1.2, nachgetestet. So konnten wir bestimmen, ob es sich um versionsspezifische- oder allgemeine Fehler handelt. Außerdem haben wir die Wipe-Funktion – sofern verfügbar – zusätzlich auf dem alternativen Testgerät durchgeführt um das Löschen von Daten auf der externen SD Karte zu verifizieren. Dies ist notwendig, da das Nexus 5 keine Möglichkeit bietet den internen Speicher mit SD Karten zu erweitern.

Allgemein konnten wir feststellen, dass es unter der aktuellen Android Version 4.4 durchwegs Probleme beim Blockieren von SMS gibt. Kein Sicherheitsprodukt konnte damit umgehen. Von vielen Herstellern wird dies auch entsprechend so kommuniziert. SMS können unter Android 4.4 nicht mehr unterdrückt oder unsichtbar gemacht werden. Problematisch wird dieser Zustand vor allem bei Produkten, die bei der Diebstahlsicherung auf SMS Kommandos setzen. Diebe können so die Befehle in SMS Form im Klartext einsehen und so an das Passwort gelangen. Wir empfehlen als erstes Kommando einen Sperrbefehl abzusetzen bevor weitere Aktionen wie Löschen oder Lokalisieren durchgeführt werden. Nur so kann der Nutzer sichergehen, dass der Dieb keinen Zugriff mehr auf die SMS Applikation besitzt.

[1] http://www.dw.de/2013-%C3%BCber-eine-milliarde-smartphones-verkauft/a-17391228

[2] https://fb-public.app.box.com/s/3iq5x6uwnqtq7ki4q8wk

Securitysoftware für Android erfordert in der Regel eine sehr große Anzahl an Berechtigungen, welche sie auf dem Smartphone erteilt bekommen. Zwischen den einzelnen Produkten konnten wir teilweise große Unterschiede ausmachen. Wir haben uns entschlossen im diesjährigen Bericht eine Tabelle mit allen Berechtigungen zu veröffentlichen, welche im Appendix auf Seite 98 nachgelesen werden kann.

Diebstahlsicherung

Fast alle Produkte im Test bieten eine Diebstahlsicherung an. Die wohl wichtigste Funktion ist das Sperren. Diese schützt das Smartphone mit einem Passwort und verhindert den Zugriff für Unbefugte. Aber auch das Löschen der Daten aus der Ferne gehört zum Standardrepertoire der getesteten Sicherheitsprogramme. Über eine Ortungsfunktion lässt sich das Gerät auch lokalisieren. Dies kann praktisch sein, um ein verlorengegangenes Smartphone wiederzufinden, allerdings warnen einige Hersteller explizit davor auf Verbrecherjagd zu gehen.

Für die Steuerung der Diebstahlsicherung gehen die Hersteller zwei Wege: Zum einen über SMS, wo Kommandos an das abhandengekommene Gerät gesendet werden und somit die entsprechende Funktion auslösen. Andere Produkte bieten ein Webinterface, über das die Diebstahlsicherung gesteuert werde kann. Beide Varianten haben Vor- und Nachteile. Der Vorteil der SMS Lösung ist, dass es praktisch immer funktioniert, selbst wenn sich das Gerät im Ausland befindet. Allerdings muss sich der Benutzer die Kommandos merken und ein zweites Mobiltelefon zur Hand haben. Im Gegensatz dazu, sind die Webinterfaces sehr intuitiv zu bedienen und erlauben eine einfachere Verwaltung der Geräte. Als Nachteil ist anzumerken, dass eine Internetverbindung bestehen muss, die allerdings im Ausland meist deaktiviert ist. Die Ortungsfunktion ist sehr nützlich, kann jedoch auch missbräuchlich zur Ortung von Personen verwendet werden. Es besteht die Möglichkeit, dass eine Person ein Security-Produkt auf dem Smartphone einer anderen Person installiert oder jemanden ein Mobiltelefon mit integriertem Security-Produkt mit Ortung schenkt, und ihn so jederzeit überwachen kann.

Android bietet bereits von Haus aus solide Diebstahlschutzfunktionen, welche unter dem Namen „Device Manager“ geführt werden. Der Vollständigkeit halber haben wir auch diese verfügbaren Funktionen untersucht um dem Leser über die bereits integrierte Basisfunktionalität von Android aufzuklären. Der Review der verfügbaren Komponenten kann auf Seite 133 gefunden werden.

Ein allgemeines Problem bezüglich des Diebstahlschutzes, welches wir bei einer Vielzahl von Produkten feststellen konnten, ist der Flugzeugmodus. Dieser kann selbst bei aktivierter Displaysperre aktiviert werden. Erst einmal aktiviert ist der Diebstahlschutz, welcher aus der Ferne steuerbar ist, komplett wirkungslos. Es ist nicht mehr möglich Kontakt mit dem Gerät aufzunehmen, wodurch Funktionen wie Sperren, Löschen, Orten aus der Ferne nicht mehr funktioniert. Dies trifft für beide Methoden der Steuerung (SMS / Webinterface) zu.

Malwareschutz

Mit Hilfe des Malwareschutzes werden Mobiltelefone auf Schadsoftware durchsucht und diese entsprechend gelöscht oder in Quarantäne verschoben. Um diese Funktion effizient nutzen zu können, muss der Virenschutz mit Updates auf dem neuesten Stand gehalten werden. Aufpassen muss man im Ausland, damit man mit automatischen Updates und Cloud-Scannern nicht in die Roaming-Falle tappt.

Die Resultate zur Anti-Malwareschutzleistung sind auf Seite 12 aufgelistet.

Batterieverbrauch

Am späten Nachmittag kann es schon einmal passieren, dass man sich wünscht für sein Smartphone ein kleines Kraftwerk in der Hosentasche zu haben. Durch die vielfältigen Funktionen der Telefone, können selbst die stromsparenden Chips den Stromverbrauch nicht massiv einbremsen. GPS, E-Mail, Internet und vor allem das bei den meisten Smartphones verbaute große Display haben sich zu regelrechten Stromfressern entwickelt. So kann es leicht passieren, dass man bei intensiver Verwendung bereits am Nachmittag mit leerem Akku da steht. Um dem vorzubeugen, gibt es drei Möglichkeiten: entweder verwendet man das Telefon sehr kontrolliert, führt ein mobiles Ladegerät mit um das Telefon unterwegs aufzuladen, oder trifft Vorkehrungen um den Stromverbrauch soweit wie möglich zu reduzieren.

Viele Anwender sind immer noch der Meinung, dass die Security-Software am Smartphone (Android) extrem stromhungrig ist. In unseren Tests konnten wir bei den meisten Sicherheitsprodukten nur eine vernachlässigbar geringe Reduktion der Akkulaufzeit während Alltagsaktionen feststellen. Bei Backups, Updates und Malwarescans hingegen ist eine Erhöhung des Batterieverbrauchs deutlich feststellbar. Hier bieten vor allem jene Produkte einen Vorteil, sie sich so konfigurieren lassen, dass sie die entsprechenden Operationen nur während des Aufladens durchführen.

Kurzübersicht

Das perfekte mobile Security-Produkt gibt es noch nicht. Hier gilt es, wie bei den Windows-Produkten, sich über die Vor- und Nachteile in unserem Report zu informieren und eine Vorauswahl zu treffen. Empfehlenswert ist die Installation kostenloser Testversionen der infrage kommenden Produkte, welche sich ein paar Tage lang ausprobieren lassen. Danach wird die Entscheidung leichter fallen. Gerade im Bereich der Android-Security-Produkte werden sehr schnell neue Versionen veröffentlicht, die Verbesserungen und neue Funktionen beinhalten.

Mit der Teilnahme am Test haben die Hersteller ihr Engagement bewiesen, gute mobile Sicherheitssoftware für ihre Kunden zur Verfügung zu stellen. Wie in diesem Report zu lesen ist, haben wir bei vielen Produkten noch Fehler oder Funktionen gefunden, die nicht einwandfrei arbeiten. Die betroffenen Hersteller nehmen diese Probleme sehr ernst und arbeiten bereits an Lösungen. Insgesamt haben wir im Vergleich zum letztjährigen Test eine deutliche Steigerung hinsichtlich der Qualität der Produkte feststellen können. Deshalb freuen wir uns, beinahe allen teilnehmenden Produkten den „Approved Award“ überreichen zu dürfen. Bedauerlicherweise gilt dies nicht für das Sicherheits-App von Tencent, welches aufgrund der Erkennungsraten beim Malwareschutz abgewertet werden muss. Qihoo wurde auch nicht zertifiziert, da das getestete Produkt nicht mehr erhältlich ist und von der im Google playstore erhältlichen Version abweicht.

AhnLab V3 Mobile ist ein Sicherheitsprodukt für Android, das die wichtigsten Sicherheitsfunktionen für Smartphones bietet. Zudem werden Funktionen wie Dateiverschlüsselung und ein Netzwerkmonitor geboten.

Ein sehr umfangreiches Sicherheitsprodukt mit einer Vielzahl an Einstellmöglichkeiten erhält der Nutzer mit **avast! Mobile Security**. Die diesjährige Version wurde mit Applocker und Privacy Scan erweitert.

Avira Antivirus Security ist ein sehr schickes Security-App für Android Smartphones und bietet alle wichtigen Funktionen. Der Diebstahlschutz wird über ein Webinterface gesteuert. Innovative Komponenten wie der Identity Safeguard runden die Software ab.

Baidu Mobile Security ist ein sehr einfach zu verwendendes Sicherheitsprodukt für Android Smartphones. Es bietet viele Funktionen, wie etwa Optimierungsfunktionen, App Manager und Anti Spam.

Bitdefender Mobile Security wurde im Vergleich zum letzten Jahr optisch überarbeitet und mit einem App Blocker ausgestattet. Die Funktionen sind durchdacht und haben im Allgemeinen sehr gut funktioniert.

CheetahMobile setzt mit der Software **Clean Master** auf die Bereinigung des Mobiltelefons. Neben einem Virenscanner werden auch andere Funktionen wie RAM- und Telefonspeicherbereinigung geboten.

CheetahMobile CM Security ist ein solide implementiertes Sicherheitsprodukt für Android Smartphones, welches wichtige Funktionen wie Antivirus und Diebstahlschutz bietet.

ESET Mobile Security bietet ein durchdachtes und schön gestaltetes App für Android Smartphones. Die Funktionen wurden solide implementiert und konnten überzeugen. Die diesjährige Version wurde mit einem Webinterface für den Diebstahlschutz erweitert.

Bei **F-Secure Mobile Security** handelt es sich um eine Sicherheitssoftware welche wichtige Sicherheitsfunktionen wie Diebstahlschutz und Virenscanner bietet. Zudem wird eine Kindersicherung und sicheres Surfen geboten.

G Data Internet Security bietet neben dem Standardrepertoire auch ausgefeilten Schutz für Kinder. So ist ein Kid's Browser, ein Children's corner und weitere Funktionen, welche hilfreich für den Schutz von Kindern sein können, inkludiert.

IKARUS mobile.security enthält alle wichtigen Sicherheitsfunktionen. Die Benutzeroberfläche wirkt aufgeräumt und sollte von jedem bedient werden können. Die implementierten Komponenten haben allgemein vernünftig funktioniert.

Kaspersky Internet Security wurde im Vergleich zur Vorjahresversion optisch überarbeitet. Der Funktionsumfang ist groß, so werden neben einem Virenscanner auch SMS & Call Filter, Browserschutz, Diebstahlschutz und mehr geboten.

Kingsoft Mobile Security für Android ist kostenlos verfügbar und optisch sehr einfach gehalten. Es werden neben den klassischen Virenschutzfunktionen auch Zusatzfeatures wie Spam Filter für SMS und Batterieschutzfunktionen.

McAfee Mobile Security bietet eine ausgereifte Software, die neben gängigen Features auch innovative Funktionen, wie eine CaptureCam und einen Kid's Corner bietet.

Quick Heal Total Security, ein App welches bereits im Vorjahr großen Funktionsumfang geboten hat, gehört auch in diesem Jahr zu den umfangreichsten Produkten. Zudem wurde bei der aktuellen Version optisch stark nachgearbeitet.

Qihoo 360 AntiVirus, welches im Vorjahr nur auf Chinesisch verfügbar war, nimmt im diesjährigen Test mit der neuen englischsprachigen Version teil. Es werden wichtige Funktionen wie Virenschutz, sowie innovative wie Anti Adware geboten. Das erreichte Ergebnis in diesem Test ist nicht übertragbar auf die englische Produktversion die im Google playstore verfügbar ist. Qihoo hat diese Auszeichnung in ihren entsprechenden Pressemitteilungen missbraucht und daher wird diese Auszeichnung zurückgezogen.

Sophos Security and Antivirus bietet viele sinnvolle Funktionen die aktiv zur Sicherheit des Nutzers beitragen. Erwähnenswert ist der Security Advisor, welcher auf mögliche kritische Einstellungen hinweist, sowie eine gut gestaltete Spam Protection Komponente.

Mobile Security von **Trend Micro** bietet neben den wichtigsten Schutzfunktionen wie dem Diebstahlschutz und Malwarescanner zusätzlich sinnvolle Erweiterungen wie sicheres Surfen und schön gestalteter Kindersicherung.

Tencent Mobile Manager ist ein Sicherheitsprodukt für Android mit einem großen Funktionsumfang. Zudem ist eine große Anzahl an optionalen Add-Ons Verfügbar, welche das Produkt noch erweitern können. Wegen des Resultats im Malware-Protection Test, der laut Tencent auf einem Bug zum Zeitpunkt des Test im Produkt bestanden hat, können wir leider keinen Approved-Award verleihen.

Webroot SecureAnywhere Mobile Complete kann mit verlässlichem Diebstahlschutz sowie mit SMS & Call Filter punkten. In der Premiumversion sind zudem SIM Lock, App Inspektoren und mehr verfügbar.

Getestete Produkte

Die 20 unten angeführten Produkte wurden in diesem Report getestet. Die Hersteller stellten entweder die neueste Produktversion zur Verfügung oder bestätigten, dass die neueste Produktversion im Google Playstore am aktuellsten Stand zum Zeitpunkt des Tests war (Juli 2014). Die Hersteller hatten nach dem Test die Gelegenheit, die gefundenen Fehler, die wir ihnen gemeldet hatten, zu beheben. Falls Sie diese Fehler behoben haben, haben wir dies im Report angemerkt.

- AhnLab V3 Mobile 2.1.2.13
- avast! Mobile Security 3.0.7650
- Avira Antivirus Security 3.5.2983
- Baidu Mobile Manager 5.2.0
- Bitdefender Mobile Security 2.19.344
- CheetahMobile Clean Master 5.6.0
- CheetahMobile CM Security 1.6.1
- ESET Mobile Security 3.0.937.0-15
- F-Secure Mobile Security 9.2.15183
- G Data Internet Security 25.3.0
- IKARUS mobile.security 1.7.20
- Kaspersky Internet Security 11.4.4.232
- Kingsoft Mobile Security 3.3.1
- McAfee Mobile Security 4.1.0.543
- Qihoo 360 AntiVirus 1.0.0
- Quick Heal Total Security 2.00.021
- Sophos Security and Antivirus 3.5.1324
- Tencent Mobile Manager 4.8.2
- Trend Micro Mobile Security 5.0
- Webroot SecureAnywhere Mobile Complete 3.6.0.6610

Die mobilen Produkte von **Baidu**, **Kingsoft**, und **Tencent** sind derzeit nur auf Chinesisch verfügbar. Die englischsprachige Version von **Qihoo** im Google Play Store ist nicht ident mit der Version die Qihoo auf der Firmenwebseite in Englisch und Chinesisch anbietet – die Ergebnisse können daher nicht auf die Google playstore Version übertragen werden.

Eine umfangreiche Übersicht der am Markt erhältlichen mobilen Produkte ist auf unserer Webseite auf http://www.av-comparatives.org/list-mobile/ verfügbar.

Batterieverbrauch

Den Batterieverbrauch eines Gerätes zu messen, scheint auf den ersten Blick sehr einfach zu sein. Geht man jedoch in die Tiefe, sieht man sehr schnell die Schwierigkeiten, die sich ergeben. Gerade bei Mobiltelefonen unterscheidet sich die Nutzung der einzelnen Anwender sehr stark. Manche legen starken Wert auf Multimedia, andere auf das Betrachten von Dokumenten, andere verwenden fast ausschließlich die Telefonfunktionen. Wir müssen hier zwischen Powerusern, die das Telefon wirklich in seinen ganzen technischen Eigenschaften ausreizen und Usern, die das Telefon nur als Mittel zum Zweck, sprich telefonieren, unterscheiden.

Für die Erstellung der Testprozedur, hat AV-Comparatives im April 2012 eine Umfrage durchgeführt, um die durchschnittliche Nutzung von Smartphones zu ermitteln. Über tausend Smartphone-Benutzer aus der ganzen Welt wurden anonym zum Thema Mobiltelefonnutzung befragt. Hier stellte sich heraus, dass die Smartphone-Nutzer die Möglichkeit ihres Telefons sehr gut ausnützen. 95% aller Smartphone Nutzer surfen und mailen mit ihrem Telefon, über 2/3 hören online Musik oder schauen sich Videos im Internet über ihr mobiles Endgerät an. Auffallend ist auch, dass 70% der User ihr Telefon nie abschalten.

Das Smartphone wird für die Anwender immer wichtiger, fast kein Benutzer lässt eine Funktion ungenutzt. Das Telefon als allgegenwärtiges Kommunikationsmittel rückt immer mehr als Ergänzung, teilweise schon als Computerersatz in den Mittelpunkt.

Die Telefonie rückt beim Smartphone eher in den Hintergrund, mehr als 41% der User verwenden ihr Telefon nur 1-10 Minuten am Tag für Gespräche. Die meisten sind länger im Internet - über 29% länger als eine Stunde am Tag.

Die Werte aus unserer Mobile Security Umfrage (April 2012) haben wir als Basis für unsere Nutzungsstatistik verwendet. Anhand der daraus gewonnenen Daten haben wir den Einfluss der Security Software auf den Batterieverbrauch der einzelnen Smartphones auf einen Durchschnittsverbrauch berechnet.

Umgebungsbedingungen

Um den Batterieverbrauch des Telefons (Battery-Drain) exakt zu messen, haben wir in Zusammenarbeit mit der Firma x.test und Agilent ein ISO-kalibriertes Messgerät in unser Labor gestellt. Mit diesem hochpräzisen Messgerät ist es möglich, den Batterieverbrauch von Geräten exakt zu messen. Mit einem standardautomatisierten Ablauf, der den User exakt nach den Umfragedaten emuliert, wurden auf dem Gerät mehrere Testläufe durchgeführt.

Äußere Einflüsse

Um äußere Einflüsse, Umwelteinflüsse als auch Einflüsse durch technische Gegebenheiten auszuschließen, wurde von uns darauf geachtet, dass jedes Gerät unter denselben Bedingungen getestet wurde. So wurde z.B. sichergestellt, dass jedes Gerät unter den gleichen Umweltbedingungen, kompatibel mit ECMA-383[3] getestet wurde.

Die 3G-Verbindung und die Wi-Fi Verbindung unterliegen Schwankungen hervorgerufen durch z.B. verschiedene Wetterlagen. Um solche Fluktuationen im Energieverbrauch zu minimieren bzw. auszuschließen, haben wir eine eigene Wi-Fi Basisstation und eine eigene UMTS Basisstation in unserem Labor aufgestellt. Hier konnten wir sicherstellen, dass die Stromaufnahme zur Herstellung einer Drahtlosverbindung für jedes Produkt gleich war.

Diese Werte sind natürlich auch vom eingesetzten Mobiltelefon abhängig. Verschiedene Faktoren beeinflussen den Energieverbrauch. So benötigt z.B. ein größeres Display mehr Leistung als ein kleines. Auch die Art des Display (LCD, OLED, AMOLED, usw.) nimmt Einfluss auf den

[3] http://www.ecma-international.org/publications/files/ECMA-ST/ECMA-383.pdf

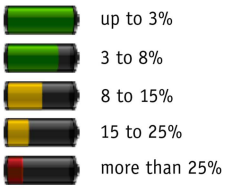
Leistungsverbrauch. Durch die Verwendung desselben Telefons für alle Testkandidaten haben wir diese Unterschiede ausgeschlossen.

Basierend auf den Umfragedaten wurden für die Batterieverbrauchsmessung folgende Nutzungsszenarien erhoben:

- **Telefonie** (30 Minuten pro Tag)
- **Bilder betrachten** (82 Minuten pro Tag)
- **Surfen im Internet** mit Android Browser, Webseite auf lokalem Webserver um Einflüsse der Verbindungsgeschwindigkeit ausschließen zu können (45 Minuten pro Tag)
- **YouTube Video mit YouTube App abspielen** (17 Minuten pro Tag)
- **Lokal gespeicherte Videos abspielen** (13 Minuten pro Tag)
- **Empfangen und Senden von Mails** unter Verwendung des Google Mail Clients (2 Minuten pro Tag)
- **Öffnen von lokalen Dokumenten** (1 Minute pro Tag)

In unserem Test konnten wir feststellen, dass die meisten mobilen Sicherheitsprodukte nur einen geringen Einfluss auf die Batterielaufzeit haben.

Hersteller	Batterieverbrauch	Hersteller	Batterieverbrauch
AhnLab		Ikarus	
avast!		Kaspersky Lab	
Avira		Kingsoft	
Baidu		McAfee	
Bitdefender		Qihoo	
Cheetah C.M.		Quick Heal	
Cheetah CM S.		Sophos	
ESET		Tencent	
F-Secure		Trend Micro	
G Data		Webroot	



Grundsätzlich dürfen wir den Herstellern der Security-Suites gute Noten ausstellen. Im diesjährigen Battery-Drain Test hat es jedoch ein Produkt gegeben, welchem wir einen erhöhten Batterieverbrauch nachweisen konnten: **Baidu**. Wir konnten jedoch keine bestimmten Operationen ausmachen, bei welcher das Produkt mehr Strom verbraucht. Der Stromverbrauch war über die gesamte Messdauer höher.

Schutz vor Android-Schädlingen

Die Methoden der Angriffe auf das Mobiltelefon werden immer raffinierter. Mit betrügerischen Applikationen werden die Benutzer von Mobiltelefon gerne um Daten oder gar Geld betrogen. Damit ihnen das nicht so leicht passiert und Sie die Gefahr auf ein Minimum reduzieren, sollten sie u.a. folgende Punkt beachten: Laden Sie Apps nur von vertrauenswürdigen Quellen herunter wie z.B. Google-Play oder den Playstores des eigenen Anbieters. Vermeiden Sie die Playstores von Drittanbietern oder auch durch Sideloading[4]. Ein weiteres Indiz unseriöse Apps aufzudecken, sind z.B. die Rechte, die die App verlangt. Als Beispiel: eine Applikation, die die Geschwindigkeit per GPS misst (z.B. im Auto) benötigt keine Rechte um das Telefonbuch oder die Telefonprotokolle einzusehen. Selbstverständlich ist es nur ein Indiz und keine Bestätigung, dass diese Applikation bösartig sein könnte, aber es sollte Sie sensibilisieren und anregen, einen zweiten Blick darauf zu werfen. Auch die Bewertungen im App Store sind eine gute Richtlinie; vermeiden Sie Applikationen mit schlechten oder dubiosen Bewertungen. Ein gerootetes Telefon bietet Ihnen zwar mehr Möglichkeiten, aber gleichzeitig ist es für bösartige Applikationen leichter, die Kontrolle über ihr Smartphone zu übernehmen. Rechtlich ist es nicht klar, ob die Garantie für das Telefon noch aufrecht ist, wenn das Telefon gerootet wurde. In vielen Fällen wird die Garantie erlöschen.

Wie hoch ist die Gefahr sich am Android Mobiltelefon zu infizieren?

Diese Frage lässt sich schwer beantworten, sie hängt von vielen verschiedenen Faktoren ab. In westlichen Ländern, bei Benutzung der offiziellen Stores wie Google-Play ist das Risiko geringer, als in Asien. In Asien, insbesondere in China, gibt es sehr viele gerootete Telefone und viele inoffizielle Appstores. In den von Google nicht überwachten Appstores ist das Gefahrenpotenzial eine infizierte App zu erwischen höher, als in den offiziellen Appstores. Auch wird in Asien das Smartphone oft als Computerersatz verwendet sowie sehr stark im Online-Banking eingesetzt. Auch in Europa und den USA sind Online-Banking Apps im Vormarsch. In den westlichen Ländern ist das Risiko, wenn man sich an die offiziellen Stores mit ungerooteten Geräten hält, momentan noch relativ gering. Man muss aber auch ausdrücklich dazu sagen, dass „geringes Risiko“ nicht gleichzusetzen ist mit „kein Risiko“. Die Bedrohungslage kann sich schnell und dramatisch ändern. Für diesen Fall sollte man bereits gewappnet sein und eine Sicherheitssoftware auf dem Mobiltelefon installiert haben. Viel wichtiger und nützlicher als der Malwareschutz am Mobiletelefon ist aus unserer Sicht zurzeit der Schutz gegen den Datenverlust bei Verlust oder Diebstahl des Smartphones.

AVC UnDroid Analyser

An dieser Stelle dürfen wir auf unser neues System hinweisen, AVC UnDroid, welches Usern kostenlos zur Verfügung gestellt wird. Hierbei handelt es sich um ein statisches Analysetool zum Erkennen von verdächtiger Schadsoftware in Android Apps (APK Dateien) und bietet zudem umfangreiche Statistiken zu Android Malware und Adware.
Nutzer können APK-Dateien hochladen und anschließend das Resultat verschiedenster Analysemechanismen einsehen.

Interessierte sind herzlich dazu eingeladen das System auf http://www.av-comparatives.org/avc-analyzer/ auszuprobieren.

[4] http://en.wikipedia.org/wiki/Sideloading

Test Set

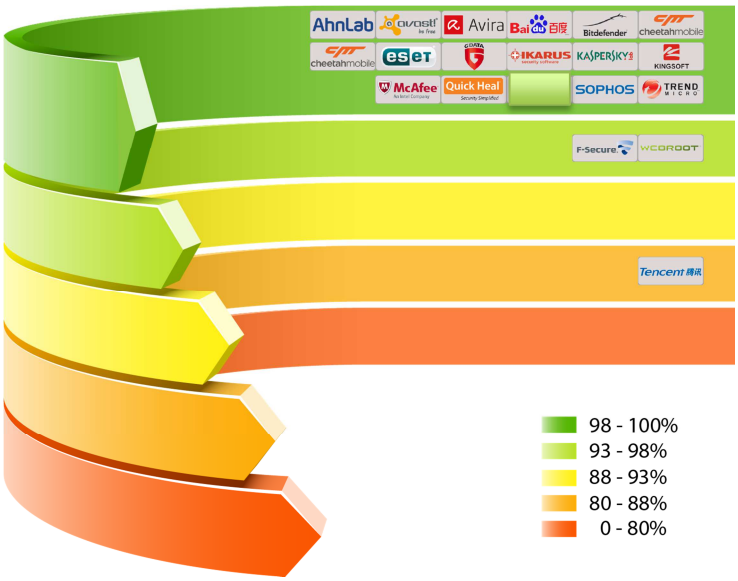
Die eingesetzte Malware wurde von uns in den letzten Monaten vor Testbeginn gesammelt. Für die Erstellung eines repräsentativen Test Sets wurden **3991** bösartige Applikationen herangenommen. Sogenannte „potentiell unerwünschte Apps" wurden nicht ins Test-Set aufgenommen. Die Sicherheitsprodukte[5] wurden am 11. Juli 2014 zuletzt aktualisiert und getestet.

Der Test wurde mit aktiver Internetverbindung auf echten Android Smartphones durchgeführt (es wurden keine Emulatoren verwendet). Das Test Set bestand ausschließlich aus APK-Dateien. Nach einem On-Demand Scan wurde jede einzelne verbleibende Malware-App manuell installiert. Wir haben uns für diese Vorgehensweise entschlossen um Produkten die Möglichkeit zu bieten Malware mittels Echtzeitscanner zu erkennen.

Auch ein Fehlalarmtest wurde von uns gegen den Top 100 (nicht werbeunterstützte) Google Play Apps durchgeführt. Keines der getesteten Produkte hatte einen Fehlalarm auf diesen 100 Applikationen.

Erkennungsraten / Ergebnisse

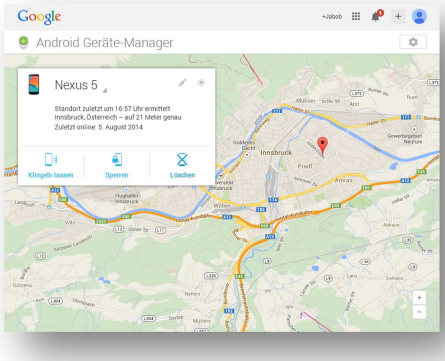
1. AhnLab, G Data 100%
2. Avira, Bitdefender, McAfee, Cheetah Clean Master, Cheetah CM Security, Kingsoft, Trend Micro 99,9%
3. Avast 99,8%
4. ESET, Kaspersky Lab 99,7%
5. Quick Heal 99,5%
6. Ikarus 98,9%
7. Baidu, Sophos 98,8%
8. Webroot 97,4%
9. F-Secure 96,1%
10. Tencent 83,8%



[5] Die Resultate von Qihoo in diesem Test sind nicht auf die im Google Play Store erhältlichen Version übertragbar, da diese zu der hier getesteten Version Unterschiede aufweist. Daher werden sie hier nicht angezeigt.

Android Device Manager

Der Android Device Manager bietet dem Nutzer solide Basisfunktionalität betreffend dem Diebstahlschutz und ist in Android standardmäßig installiert. Die Steuerung dieser Komponente findet über ein Webinterface (https://www.google.com/android/devicemanager) statt. SMS Kommandos werden nicht angeboten.



Installation

Die Installation des Schutzes entfällt, da sie bereits in Android integriert ist. Auf unserem Testgerät war die Funktion bereits standardmäßig aktiviert. Gegebenenfalls muss sie über „Google Settings > Android Device Manager“ aktiviert werden.

Orten

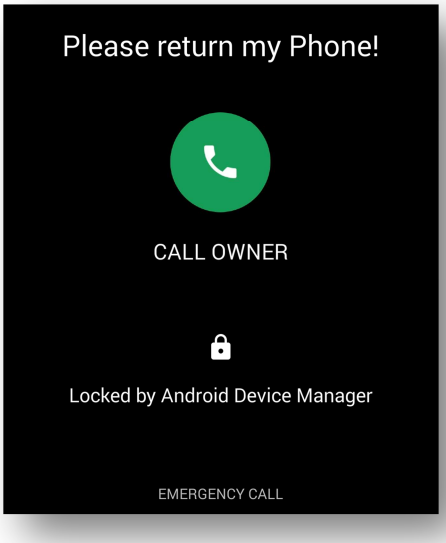
Diese Funktion ortet ein gestohlenes oder verlorengegangenes Gerät und zeigt die Position auf einer Karte von Google Maps an. Die Positionierung erfolgt jeweils nur einmalig – ein Aufzeichnen eines Bewegungsprofils wird nicht angeboten.

Klingeln Lassen

Die Klingeln Lassen Funktion lässt für fünf Minuten eine Melodie auf höchster Lautstärke ertönen. Hierbei handelt es sich um eine Funktion, welche zum Beispiel helfen kann ein verlegtes Handy innerhalb der eigenen vier Wände wiederzufinden. Das Gerät wird durch Absetzen des Kommandos nicht gesperrt.

Sperren

Die Sperren-Funktion sperrt das Gerät mit dem Android Sperrbildschirm. So soll der Zugriff für Unbefugte unmöglich gemacht werden. Im Webinterface kann das Passwort für die Sperre direkt festgelegt werden. Gefallen hat uns, dass auf dem Sperrbildschirm eine Nachricht angezeigt werden kann, welche ebenfalls im Webinterface definierbar ist. Ein Anwendungsfall wäre etwa einem ehrlichen Finder Informationen zu geben wie er den Besitzer kontaktieren kann um das Gerät zurückzugeben. Zusätzlich kann eine Telefonnummer angegeben werden, die es Findern erlaubt direkt Kontakt mit dem Besitzer aufzunehmen. Über den Sperrbildschirm kann diese Nummer (nur diese) angerufen werden.



In unserem Test war die Sperrfunktion solide implementiert. Wir konnten sie nicht umgehen und hatten zu jedem Zeitpunkt die Möglichkeit einen Notruf abzusetzen.

Löschen

Diese Funktion löscht die persönlichen Daten vom Smartphone des Nutzers. Nach dem Absetzen des Befehls wird das Gerät auf Werkseinstellungen zurückgesetzt. Google weist darauf hin, dass bei manchen Geräten die SD Karte unter Umständen nicht gelöscht wird. Dies konnten wir in unseren Tests bestätigen. Während auf dem Nexus 5 alle

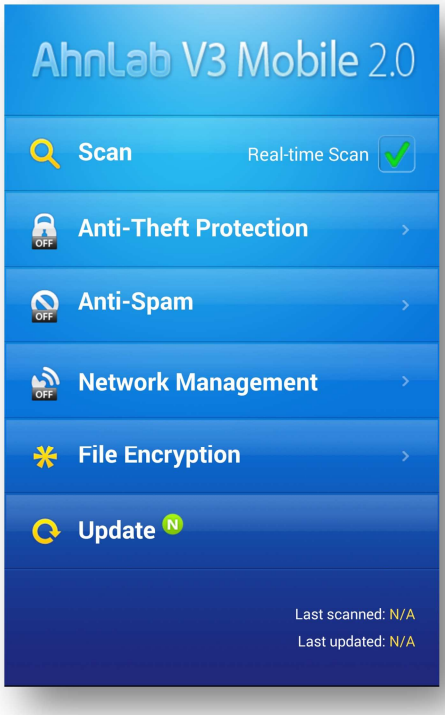
Daten gelöscht wurden, blieben die Files auf der externen SD-Karte des alternativen Testgeräts unangetastet.

Fazit

Der Android Device Manager von Google bietet keinen sehr großen Funktionsumfang, hat jedoch alle vorhandenen Komponenten durchwegs solide implementiert. Für Nutzer, welche vorwiegend wegen dem Diebstahlschutz überlegen ein mobiles Sicherheitsprodukt einzusetzen kann der Android Device Manager ausreichend und eine gute Wahl sein.

AhnLab V3 Mobile

AhnLab bietet mit AhnLab V3 Mobile ein Sicherheitsprodukt für Android, das die wichtigsten Sicherheitsfeatures, wie Malwarescanner, Diebstahlschutz und Anti-Spam beinhaltet.



Installation

AhnLab V3 Mobile wurde uns von AhnLab als APK-Datei zur Verfügung gestellt. Die Installation gestaltete sich einfach. Nach dem Akzeptieren der Lizenzvereinbarung musste das Gerät registriert werden, was in wenigen Sekunden und ohne weitere Nutzereingaben erfolgte. Abschließend wird der Nutzer auf den Startbildschirm weitergeleitet.

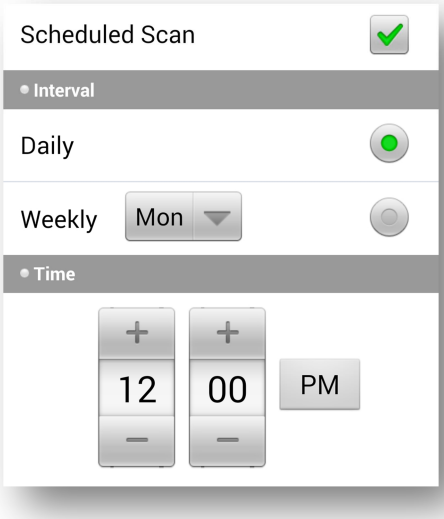
Starten des Programms

Nach der erfolgreichen Installation konnte AhnLab V3 Mobile gestartet werden. Es findet keinerlei Einführung statt, der Nutzer muss durch Probieren das Produkt erkunden. Des Weiteren findet kein initiales Update der Signaturen statt. Der standardmäßig aktivierte Echtzeitschutz lässt sich über den Homescreen direkt ein- und ausschalten, auch alle anderen Komponenten sind von dort erreichbar. Am unteren Bildschirmrand sind die Daten des letzten Scans und des letzten Updates ersichtlich. Bei beiden ist „*N/A*“ eingetragen.

Scan

Unter dem Modul Scan findet der Nutzer zwei verschiedene Varianten von Überprüfungen. Einerseits den *Smart Scan*, der alle installierten Apps auf schadhaftes Verhalten prüft, sowie den *Intense Scan*, der zusätzlich noch alle auf dem Gerät befindlichen Dateien überprüft. Außerdem werden die Daten vom letzten durchgeführten, sowie dem nächsten *Scheduled Scan*, also dem nächsten zeitgesteuerten Scan, angezeigt. Einstellungen hierfür können im globalen Einstellungsmenü getroffen werden. Neben dem Intervall (täglich und wöchentlich) kann auch der Zeitpunkt bestimmt werden.

In den Einstellungen findet sich auch eine Option, ob „Potentially Unwanted Apps“, also solche die der Nutzer möglicherweise nicht auf seinem Telefon installieren möchte, blockiert werden sollen. Als Beispiel für derartige Applikationen nennt AhnLab Adware, Spyware und Dialer.



Anti-Theft Protection

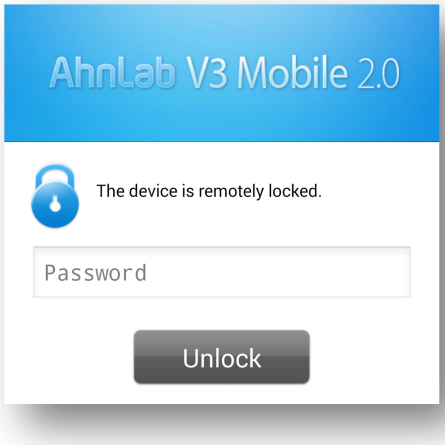
Für die Verwendung dieser Komponente wird ein Passwort vorausgesetzt, das zwischen 4 und 10 Zeichen lang sein muss. Außerdem muss das Produkt zur Aktivierung als Device Administrator eingetragen werden. Insgesamt

ist die Einrichtung sehr einfach. Die Steuerung des Diebstahlschutzes hat AhnLab über SMS Kommandos realisiert. Diese werden in einer Übersicht aufgelistet. Über eine Eingabezeile kann der Nutzer SMS Kommandos auf ihre Richtigkeit überprüfen und sofort testen. Ein Webinterface ist nicht vorhanden.

Lock

SMS Kommando:
„#lock <Passwort><Nachricht>“

Der Lock sperrt das Smartphone und soll somit vor unbefugtem Zugriff schützen. Hierfür wird das zuvor eingegebene Passwort benötigt. Gefallen hat uns, dass es möglich ist eine persönliche Nachricht am Display erscheinen zu lassen. Auch positiv anzumerken ist, dass nach zehnmaliger falscher Eingabe ein SMS mit der Position automatisch an den Sender des Sperrkommandos gesendet wird.



Negativ aufgefallen ist, dass es nach erfolgreicher Sperrung nicht möglich ist einen Notruf abzusetzen. Außerdem ist der Lockscreen nicht besonders sicher. Durch simples Betätigen des Homebuttons erscheint der Startbildschirm. Durch diesen kann navigiert und installierte Apps angezeigt werden. Auch das Starten von Programmen ist möglich, jedoch erscheint nach wenigen Sekunden wieder der Sperrbildschirm. In unserem Test konnten wir sogar zu den SMS navigieren, wo das Passwort für die Sperre ausgelesen werden kann. Die Lock Komponente erfüllt somit nicht ihren Zweck.

Remote Data Delete

SMS Kommando: „#remove <Passwort>“

Dieses Kommando löscht persönliche Daten vom Smartphone. Dabei wird das Gerät nicht auf den Werkszustand zurückgesetzt, was den Vorteil bietet, dass die Funktionen bezüglich Diebstahlschutzes aktiv bleiben. Obwohl die SMS Nachrichten nicht gelöscht wurden, war diese Komponente überwiegend zufriedenstellend. Alle Kontakte, Dateien Kalendereinträge, der Browser Verlauf & die Lesezeichen wurden gelöscht.

In einem zweiten Test auf einem anderen Gerät mit Android 4.1.2 wurden auch die SMS Nachrichten gelöscht. Jedoch wurden von der externen SD Karte keine PDF und ZIP Dateien gelöscht. Mediadateien wie JPG, MP3, MP4 und AVI jedoch schon.

Ein Großteil der gelöschten Daten von der externen SD Karte konnte mit Freewaretools wiederhergestellt werden.

Remote Wipe Reset

SMS Kommando: „#kill <Passwort>“

Mit diesem Kommando wird das Gerät auf Werkseinstellungen zurückgesetzt. Im Gegensatz zum Remote Data Delete wurden somit nach dem Absetzen des Kommandos zusätzlich die SMS Nachrichten gelöscht. Dies bringt jedoch den Nachteil mit sich, dass die Anti-Theft Komponenten nicht mehr aktiv sind.

Remote Location Tracking

SMS Kommando: „#locate <Passwort>“

Nach Absenden des Kommandos erhält der Sender prompt eine Antwort mit einem Link auf Google Maps inklusive Koordinaten. Auch wenn wir uns unter der Bezeichnung „Tracking“ ein kontinuierliches Orten über längere Zeit erwarten würden hat die Ortungsfunktion insgesamt sehr gut funktioniert.

SIM card swap

Wird die SIM-Karte ausgetauscht wird ein SMS an die von dem Benutzer eingestellte Nummer

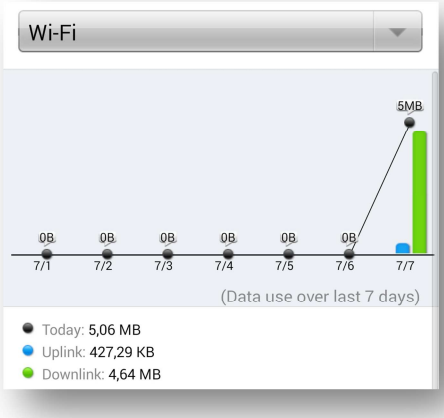
mit der Position des Telefons gesendet. Gleichzeitig wird das Gerät gesperrt.
In unserem Test hat dies nicht funktioniert. Es wurde kein SMS abgesendet, gesperrt wurde das Gerät auch nicht. In einem zweiten Test mit einem anderen Gerät mit Android 4.1.2 funktionierte alles wie erwartet.

Anti-Spam

Die Anti-Spam Komponente von AhnLab ermöglicht das Blacklisting von Telefonnummern für SMS und Anrufe. Für das Hinzufügen von neuen Nummern werden dem Nutzer mehrere Möglichkeiten geboten: Aus dem Telefon und SMS Log, aus den Kontakten oder per manueller Eingabe. Für jede Nummer kann bestimmt werden, ob nur SMS, Anrufe oder beides gefiltert werden sollen.
Weiters können SMS entsprechend dem Inhalt geblockt werden. Hierfür können Keywords mit einer Länge von zwei bis zehn Zeichen definiert werden. Warum die Länge nach oben hin beschränkt ist, ist uns unklar. In einem Untermenü können alle bisher geblockten Anrufe und SMS angezeigt werden. Außerdem ist die Blockierung Case-Sensitiv was in unseren Augen für eine derartige Funktion sinnlos ist.
Insgesamt ist die Anti-Spam Komponente schick und übersichtlich gestaltet. Die Blockierung von Anrufen hat auch tadellos funktioniert. Die Blockierung von SMS hat im diesjährigen Test jedoch nicht funktioniert. Offensichtlich scheint der Hersteller noch Probleme mit der getesteten Android Version (4.4.2) zu haben. In einem zweiten Test mit einem anderen Gerät (Android 4.1.2) wurden die SMS wie erwartet blockiert.

Network Management

Unter Network Management fasst AhnLab Funktionen, die das Netzwerk betreffen zusammen.
Beim Verbinden mit einem WiFi Hotspot erscheint ein Pop-Up, das dem Nutzer ermöglicht das WiFi zu deaktivieren, den Zugriff auf den Hotspot dauerhaft zu gewähren oder zu unterbinden. Über Listen können die bekannten Access Points verwaltet werden.
Der Datenverbrauch über mobile Netzwerke kann eingeschränkt werden. Wenn der Verbrauch ein definiertes Limit erreicht, wird der Nutzer gewarnt. Unter der Registerkarte *Network Monitoring* erhält der Nutzer Statistiken zu seiner Datennutzung. Diese kann nach mobilem- und WLAN Traffic aufgeschlüsselt werden. Außerdem werden die Datenmengen für Up- und Download separat für verschiedene Zeitintervalle angezeigt.



File Encryption

File Encryption ermöglicht die Verschlüsselung von einzelnen Dateien. Über einen Explorer können mehrere Files ausgewählt werden und mit einem vier bis zehn alphanummerischen Zeichen langen Passwort verschlüsselt werden. Resultat ist eine Datei mit Endung *.aed, welche sich nicht mehr öffnen lässt. Auch das Entschlüsseln findet über die AhnLab Anwendung statt. Es gibt keine Einschränkungen bezüglich dem Dateityp der Ursprungsdatei, so können Bilder, Videos, PDFs etc. verschlüsselt werden. In unserem Test wurden die Dateien zwar korrekt ver- und entschlüsselt, jedoch ist die Applikation nach jedem Vorgang abgestürzt.

Updates

Können nach einem Zeitplan automatisiert, oder manuell durchgeführt werden. Hierbei kann der Nutzer entscheiden ob diese nur

über WiFi oder auch über das Mobilfunknetz geladen werden.

Hilfe

AhnLab bietet dem Nutzer eine Hilfe, die sehr schön kategorisiert ist. Gefallen hat uns, dass eine Schritt für Schritt Anleitung existiert. Nervig ist allerdings, dass man durch Drücken des Zurückbuttons immer auf den Startbildschirm bzw. zum Start der Hilfe geleitet wird. Außerdem kann nicht gezoomt werden, wodurch der gesamte Text sehr klein dargestellt wird.

Deinstallation

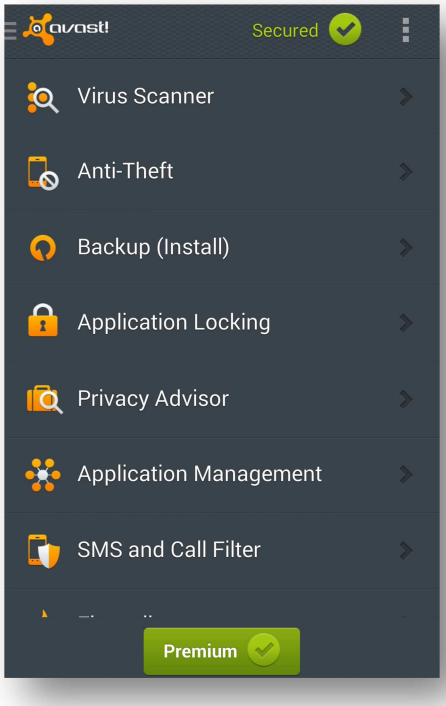
Es gibt keinen Assistenten zum Deinstallieren der Software, jedoch befindet sich eine Schritt-für-Schritt Anleitung in der Hilfe. Als erstes muss AhnLab bei den Device Administratoren ausgetragen werden. Anschließend kann das Programm über den Android App Manager deinstalliert werden.
Für die Deinstallation war keine Passworteingabe nötig, was ein Sicherheitsrisiko darstellt, da ein Dieb den Diebstahlschutz auf diese Art und Weise einfach deinstallieren kann.

Fazit

AhnLab V3 Mobile bietet die wichtigsten Sicherheitsfunktionen für Android Smartphones. Neben den klassischen Schutzmechanismen wie dem Diebstahlschutz gefallen auch innovative Funktionen wie die Dateiverschlüsselung und das Networkmanagement. Offensichtlich hat AhnLab noch Probleme mit der neuen Android Version. So konnten wir Patzer bei AntiSpam, Lockscreen und Fileencryption feststellen.

avast! Mobile Security

Avast bietet mit avast! Mobile Security ein umfangreiches Sicherheitsprodukt für Mobiltelefone und Tablets kostenlos an. Zu den wichtigsten Funktionen zählen ein Antiviren- und Browserschutz sowie eine Diebstahlsicherung.



Installation

Avast Mobile Security wurde aus dem Google Play Store bezogen und installiert. Der Nutzer wird durch eine Einführung geleitet, die die wichtigsten Funktionen auflistet. Anschließend empfiehlt Avast die Durchführung eines Scans aller installierten Applikationen. Dieser Schritt kann jedoch übersprungen werden. Im Zuge dessen wird ein Update der Virendefinitionen durchgeführt.

Starten des Programms

Beim ersten Start des Programms wird der Homescreen angezeigt, welcher den großen Umfang des Produkts bereits erahnen lässt. Am unteren Ende des Bildschirms ist ein „Go Premium“ Button eingeblendet.
Die Navigation durch die Menüs gestaltet sich überwiegend intuitiv.

Virus Scanner

Der Virusscanner scannt alle installierten Anwendungen auf Malware. Optional hat der Nutzer die Möglichkeit, die Überprüfung von Dateien zu aktivieren. Durch langes Halten auf dieser Checkbox erscheint ein Auswahlmenü, über das ein spezifischer Ordner angegeben werden kann, welcher gescannt werden soll. Am unteren Bildschirmrand werden Buttons eingeblendet, über die ein automatischer Scan konfiguriert werden kann. Neben den Wochentagen kann auch die Uhrzeit des Scans eingestellt werden.

Shield Control

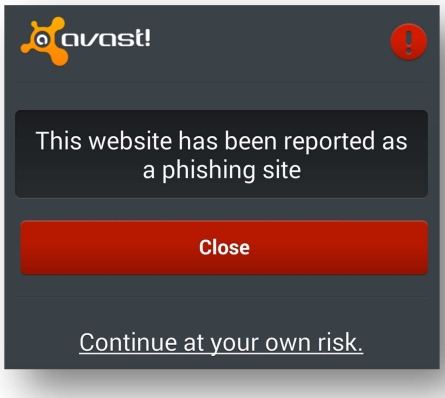
Verschiedenste Echtzeitschutzfunktionen werden bei Avast als *Shield* bezeichnet. Die verfügbaren Shields sind durch Wischen nach rechts erreichbar. Folgende Shields sind verfügbar:

App Shield

Das *App Shield* scannt je nach Einstellungen Apps während der Installation oder ihrer Ausführung.

Web Shield

Diese Komponente schützt den Nutzer während dem Surfen vor Phishingseiten oder jenen, die Schadcode enthalten. Hierbei wird sowohl der Standardbrowser, als auch Google Chrome, Amazon Silk und Boat Browser unterstützt. Dies hat in unserem Kurztest auch sehr gut funktioniert.



Zusätzlich bietet avast einen Spelling-Checker, der bei falsch getippten URLs eingreifen soll

und diese richtig stellen soll. In unseren Tests haben wir jedoch keinen Fall produzieren können, wo Avast eingegriffen hätte.

Message Shield

Scannt alle eingehenden Nachrichten auf Phishing oder gefährliche URLs. Dies hat in unserem Test sehr sauber funktioniert. Außerdem können Nachrichten mit unbekanntem Absender blockiert werden.

File Shield

Scannt Dateien während dem Lesen oder Schreiben auf schadhaftes Verhalten. Auch dies hat in unserem Test einwandfrei funktioniert. Diese Komponente ist standardmäßig deaktiviert.

Anti Theft

Die Anti-Theft Komponente ist eine Stand-Alone Anwendung und muss nachträglich installiert werden. Dies bringt den Vorteil, dass die App versteckt werden kann. Sollte der Nutzer ein gerootetes Gerät besitzen, so kann er den Diebstahlschutz *hard-reset proof* installieren. Nach einer derartigen Installation ist der Diebstahlschutz sogar nach einem Zurücksetzen des Geräts auf Werkseinstellungen noch verfügbar.

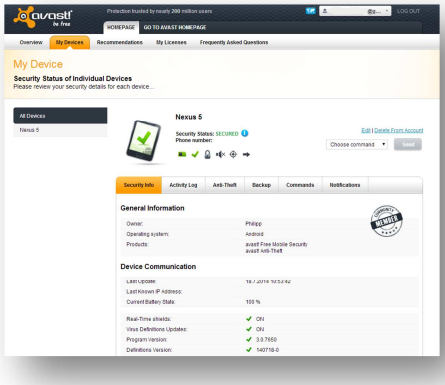
Die Installation erfordert ein einfaches, aber relativ umfangreiches Setup. So muss der Name, die Telefonnummer eines Freundes, sowie ein 4-6 stelliger PIN eingegeben werden. Anschließend muss sich der Nutzer mit seiner Emailadresse oder einem Facebook Account einloggen, sofern er auch das Webinterface verwenden möchte. Des Weiteren muss die Telefonnummer angegeben werden.

Avast bietet für Android 4.4 ein spezielles binäres SMS Format, welches notwendig ist, da ansonsten ausgehende SMS von Dieben gelesen werden könnten.

Durch die Aktivierung der Anti-Theft Komponente wird automatisch der Stealth Mode aktiviert, welcher die Diebstahlschutzfunktion komplett versteckt. Durch simples Anrufen des PINs wird die Komponente wieder sichtbar gemacht und angezeigt.

Mit einem grellen gelben Symbol wird signalisiert, dass es noch Probleme bei den Einstellungen gibt. So wird darauf hingewiesen, dass avast! als Geräteadministrator aktiviert werden muss.

Die Steuerung der Anti-Theft Komponente kann einerseits über das Webinterface (http://my.avast.com) oder einer Vielzahl von SMS Kommandos durchgeführt werden. Neben den Klassikern wie Sperren, Lokalisieren und Löschen bietet Avast z.B. auch die Weiterleitung von SMS, Anruflisten, Umleitung von Anrufen, usw. Eine Übersicht aller Befehle findet sich hier: http://www.avast.com/free-mobile-security#tab3 (auf Button „Control via SMS“ klicken).



Lock

SMS Kommando: „<PIN> LOCK“

Nach Absetzen des Kommandos wird das Gerät gesperrt und ein Lockscreen angezeigt. Ein ehrlicher Finder wird dazu aufgefordert eine Fundmeldung bei avast zu machen. Hierfür muss die IMEI, die während des Locks angezeigt wird, an android@avast.com gesendet werden. Dieser Anzeigetext kann jedoch editiert werden. Zusätzlich ertönt eine laute Sirene mit einem Ansagetext „*This phone has been lost or stolen*“. Diese ist nur in Englisch verfügbar. Durch Eingabe des richtigen PINs kann die Sperre aufgehoben werden.

Die Sperrfunktion hat in unserem Test insgesamt gut funktioniert. Wir konnten die

Sperre nicht umgehen und somit nicht auf persönliche Daten zugreifen. Ein Kritikpunkt: Wir konnten durch Halten des Einschaltknopfes den Flugzeugmodus aktivieren, wodurch weder SMS Kommandos, noch Webinterface mehr funktionieren. Des Weiteren ist es nicht möglich bei gesperrtem Smartphone einen Notruf abzusetzen, was unter Umständen gefährlich werden kann.

Siren

SMS Kommando: „<PIN> SIREN ON“

Mit diesem Kommando wird derselbe Ton wie auch schon beim Sperren abgespielt, mit dem Unterschied, dass das Gerät nicht gesperrt wird. Diese Funktion dient somit nicht der Sicherheit, sondern dem Wiederfinden des Geräts, wenn es verlegt wurde.

Locate

SMS Kommando: „<PIN> LOCATE<INTERVALL>“.

Mit diesem Kommando wird das Gerät geortet. Im Anschluss erhält der Sender eine Antwort-SMS mit einem Link auf eine Onlinekarte inklusive Koordinaten, Zellinformationen und Netzbetreiber. Durch den optionalen Parameter *Intervall*, das in Minuten angegeben wird, kann selbst über SMS ein kontinuierliches Tracken, ein Aufzeichnen des Bewegungsprofils, durchgeführt werden. Selbstverständlich hat der Nutzer auch die Möglichkeit diese Funktionalität über das Webinterface zu nutzen, wo der Bewegungsverlauf in einer Karte dargestellt wird. Diese Art der Darstellung eignet sich deutlich besser als das permanente Senden von SMS.

Die kontinuierliche Ortung kann mit dem SMS Befehl „<PIN> LOCATE STOP“ angehalten werden.

Wipe

SMS Kommando: „<PIN> WIPE“

Diese Funktion löscht persönliche Daten vom Smartphone des Nutzers. Hierfür bietet avast! mehrere Varianten an.

Bei der herkömmlichen Methode wird das Gerät nicht auf Werkseinstellungen zurückgesetzt. In unserem Test wurden persönliche Daten wie Kontakte, Lesezeichen und Kalendereinträge Dateien etc. gelöscht, jedoch nicht die SMS und der Google Account. Somit können Emails nach wie vor empfangen und gelesen werden. Auf unserem alternativen Gerät mit Android 4.1.2 wurden auch die SMS gelöscht.

Beim gründlichen Löschen wird die SD Karte mit Junk-Dateien überschrieben, was zwar um einiges länger dauert, jedoch ein Wiederherstellen der Daten verhindern soll. In unserem Test hat dies jedoch nicht funktioniert. Wir konnten mit gängigen Freewareprogrammen den Großteil der Dateien wiederherstellen.

Durch Setzen des Geräteadministrators in den Einstellungen hat Avast die Möglichkeit das Gerät bei einem Wipe auf Werkseinstellungen zurücksetzt. Bei diesem werden auch die SMS und der Google Account gelöscht, jedoch hat danach der Nutzer keine Möglichkeit mehr die Diebstahlschutzfunktionen zu verwenden.

SIM Change Lock

Avast bietet eine Funktion an, welche das Gerät sperrt, wenn die SIM Karte getauscht wird, etwa wenn ein Dieb seine eigene einlegt. Der Nutzer kann einstellen welche Aktionen in einem derartigen Fall ausgeführt werden sollen, wie zum Beispiel das Sperren des Geräts und dem Abspielen eines Sirenensignals.

Backup

Diese Funktion muss erst nachinstalliert werden und ermöglicht das Sichern persönlichen Daten. Als Speicherdienst kommt hier Google Drive zum Einsatz.

Nach der Aktivierung kann der Nutzer wählen, welche Daten gesichert werden sollen. Mit Checkboxen kann jeweils bestimmt werden, ob Alle Kontakte, Anrufe, SMS, Bilder, Audio- und Videodateien, sowie alle Apps gesichert werden sollen. Sinnvoll ist auch die Einstellmöglichkeit, dass Backups nur bei

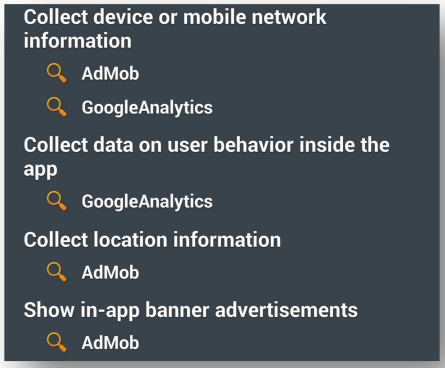
aktiver WiFi Verbindung erfolgen dürfen. Auch ein minimaler Akkustand kann eingestellt werden, der für die Durchführung eines Backups erforderlich sein soll.
In den Einstellungen können Trigger gesetzt werden, die ein Backup anstoßen. So kann etwa eingestellt werden, dass nach jedem Systemstart oder bei jedem Anstecken des Ladegeräts eine Sicherung durchgeführt wird. Zusätzlich kann das Backup mit einem Zeitplan gesteuert werden (Wochentag und Uhrzeit einstellbar).
Die gesicherten Dateien können im Webinterface von Google Drive direkt angezeigt werden. Kontakte, SMS und Anrufe werden laut Angaben von Avast nicht in Google Drive, sondern auf den Servern von Avast gespeichert.

Application Locking

Diese Funktion ermöglicht das Sperren von auswählbaren Applikationen mit einem Passwort. Avast empfiehlt den Google Play Store und die Einstellungen mit einem Passwort zu versehen. Es kann jedoch auch jede andere installierte Applikation geschützt werden.

Privacy Advisor

Der Privacy Advisor kategorisiert Anwendungen, welche spezielle Berechtigungen wie z.B. *Auf Nachrichten zugreifen, Lokalisieren* oder *Zugriff auf Kontakte* benötigen. Dadurch erhält der Anwender eine Übersicht von möglichen Datenschutzproblemen auf seinem mobilen Gerät. Durch Antippen einer der sieben Kategorien werden die Apps mit den jeweiligen Berechtigungen angezeigt. Tippt der Nutzer dann eine der Apps an, so werden detaillierte Informationen, sowie ein Button zum sofortigen Beenden des Programms angezeigt.
Zusätzlich zu den Berechtigungen bietet Avast einen Ad-Detector, welcher alle Werbenetzwerke, die in das Produkt integriert sind, anzeigt. So wird zum Beispiel Google Analytics, oder AdMob angezeigt. Zudem werden die Berechtigungen der Werbenetzwerke angezeigt. Ein Beispiel wäre, ob ein Werbenetzwerk die Berechtigung hat das Gerät zu orten, oder Werbung im Vollbildmodus oder Werbebanner anzeigt.

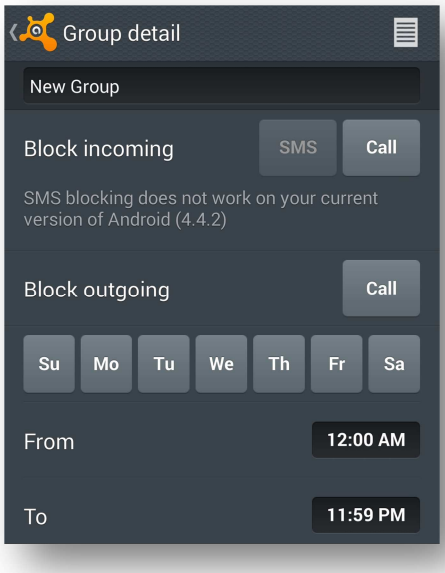


Application Management

Mithilfe des Application Managers können laufende und installierte Apps auf CPU Last, RAM, Speicher und weitere Ressourcen analysiert und beendet werden.

SMS and Call Filter

Um nicht vor ungewünschten Anrufen bzw. SMS Nachrichten gestört zu werden, bietet avast! den *SMS und Call Filter* an. Hierfür können Gruppen angelegt werden, um Anrufe und SMS Nachrichten zu gewissen Zeitpunkten von bestimmten Mitgliedern zu blockieren.



Die Mitglieder können Kontakte aus dem Adressbuch, Rufnummern, alle anonymen Anrufer und unbekannten Teilnehmern sein. Avast verfolgt bei dieser Komponente den Ansatz des Blacklistings. Es werden also all Anrufer durchgelassen, welche nicht explizit einer Gruppe zugeordnet sind.
Avast macht darauf aufmerksam, dass die Blockierung von SMS mit der Android Version nicht kompatibel ist. Auf unserem alternativen Testgerät mit Android 4.1.2 hat die Funktion jedoch wie erwartet funktioniert.

Firewall

Die Firewall ist bei nicht gerooteten Geräten deaktiviert und kann nicht verwendet werden. Dies ist durch Einschränkungen des Betriebssystems bei nicht gerooteten Geräten normal. Da wir in unseren Tests vom Szenario eines Durchschnittsnutzers ausgehen, welcher sein Gerät nicht rootet, konnten wir diese Funktion nicht testen.

Network Meter

Diese Komponente listet den das verbrauchte Datenvolumen aller installierten Apps. Hierbei kann nach WiFi, 3G, Roaming und Gesamt aufgeschlüsselt werden. Durch Antippen einer der Apps wird das Transfervolumen zusätzlich nach Datum (Heute, Monat, Jahr) aufgeschlüsselt dargestellt.

Updates

Updates werden automatisch durchgeführt. Hierfür kann gewählt werden welche Netzwerke hierfür zur Verfügung stehen sollen (Wifi, 3G, Roaming). Zusätzlich können Updates auch manuell angestoßen werden.

Hilfe

Innerhalb der Applikation existiert keine Hilfe. Dies kann vor allem in Anbetracht des großen Funktionsumfanges und Einstellmöglichkeiten problematisch sein. Auf der Webseite von Avast findet sich ein Benutzerhandbuch (34 Seiten), sowie FAQ.

Deinstallation

Die Deinstallation von avast! Mobile Security kann ohne Passworteingabe durchgeführt werden. Der Diebstahlschutz bleibt jedoch aktiv, da diese Komponente in eine separate App ausgelagert wurde. Der Passwortschutz für Apps (Application Locker) geht dadurch jedoch verloren, was die ganze Funktion ein wenig sinnlos erscheinen lässt.

Lizenz

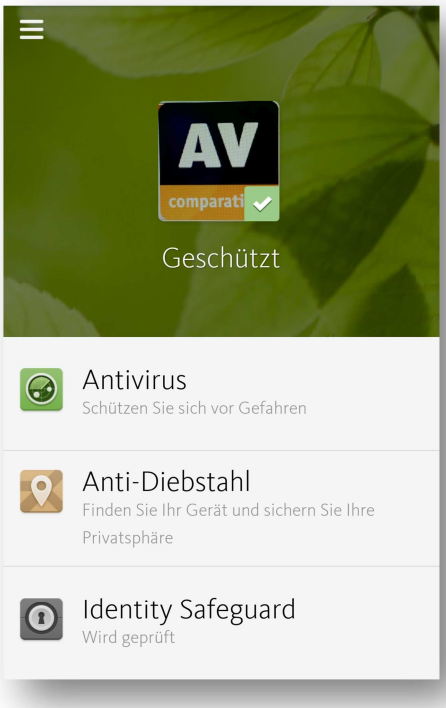
Avast Mobile Security wird in eingeschränktem Funktionsumfang kostenlos zur Verfügung gestellt. Für Premiumfunktionen wie App Locking, Ad Detector, ausgewählten Anti-Theft Features sowie der Backupfunktion muss ein Premium Plan erworben werden, welcher für 1,99€ pro Monat, oder 14,99€ pro Jahr erhältlich ist.

Fazit

avast! Mobile Security verfügt über einen großen Funktionsumfang mit innovativen Funktionen. Besonders gut gefallen hat uns die Vielzahl an Einstellungsmöglichkeiten und Remote Befehlen, welche dem Anwender eine umfassende Fernkontrolle bieten. Die im Vorjahr versprochenen Funktionen wie Backup, Applocker und Privacy Scan wurden implementiert und runden das Programm ab.

Avira Antivirus Security

Avira bietet mit Antivirus Security ein schickes Sicherheitsprodukt, welches über wichtige Sicherheitsfunktionen wie Virenscanner, Diebstahlschutz und Blockierlisten verfügt. Innovative Komponenten wie Identity Safeguard runden das Produkt ab.



Installation

Avira Antivirus Security wurde kostenlos aus dem Google Play Store bezogen und installiert. Als erster Schritt muss ein neues Konto angelegt oder ein bestehendes eingeloggt werden. Hierfür muss die Emailadresse und ein mindestens fünfstelliges Passwort angegeben werden. Anschließend empfiehlt Avira ein Foto, sowie Vor- und Nachname zu speichern, da sich mit diesen Informationen verlorene Geräte leichter wiederfinden lassen. Nach erfolgter Anmeldung wird die Antivirenkomponente des Produkts aktualisiert und anschließend ein Systemscan durchgeführt.

Starten des Programms

Beim ersten Starten des Programms erscheint ein schön gestalteter Homebildschirm. In der Mitte des oberen Bildschirmteils erscheinen das Bild des Nutzers und ein Hinweis, dass Handeln erforderlich ist. Diese Meldung wird eingeblendet, weil die Anti-Diebstahlkomponente nicht eingerichtet wurde.

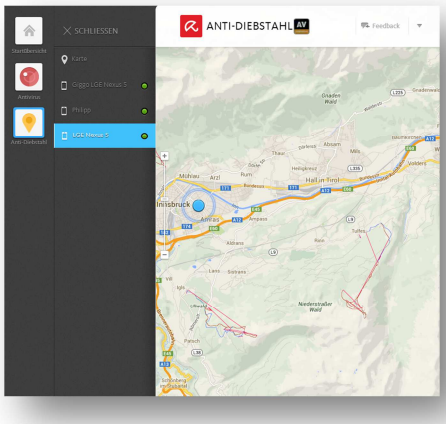
Auf dem Startbildschirm sind die wichtigsten Funktionen aufgelistet. In einem Kontextmenü, welches sich durch Wischen von links öffnen lässt, lassen sich das Profil verwalten, Einstellungen ändern und die Hilfe aufrufen.

Antivirus

Die Antivirenkomponente des Produkts kann unter dem Menüpunkt *Antivirus* gefunden werden und ermöglicht das Scannen von installierten Apps und Dateien im Dateisystem. Avira zeigt Statistiken bezüglich der Anzahl von geprüften Apps und Dateien, sowie das Datum der letzten Prüfung an. Am unteren Ende der Liste wird die Version der Virendefinition angezeigt und das Datum der nächsten automatischen Aktualisierung. Eine manuelle Aktualisierung ist nicht möglich. In den Einstellungen kann der Nutzer die zu überprüfenden Gefahrenkategorien auswählen. Hierbei ist *Adware* bereits standardmäßig aktiviert, zusätzlich kann das Scannen von PUA (Potenziell Unerwünschte Anwendungen) aktiviert werden.

Anti-Diebstahl

Die Diebstahlschutzkomponente von Avira wird über ein schön gestaltetes Webinterface gesteuert (http://my.avira.com). SMS-Kommandos sind nicht verfügbar. Das Webinterface ermöglicht es dem Nutzer mehrere Geräte in einem Nutzerkonto zu verwalten.



Im der Diebstahlschutzmodul von Avira erscheint am oberen Bildschirmrand eine Meldung, dass der Geräteadministrator deaktiviert ist. In einer Infobox wird die Erklärung angezeigt, dass die Aktivierung des Geräteadministrators notwendig ist, um die Fernlöschung durch Rücksetzen auf Werkseinstellungen zu erlauben. Des Weiteren wird angeführt, dass der Geräteadministrator für die Fernsperrung auf manchen Tablet-PCs notwendig sei. Durch Tippen auf den „Aktivieren Button" kann Avira als Geräteadministrator eingetragen werden, worauf sich der Status auf dem Startbildschirm auf „Geschützt" ändert.

Ton abspielen

Die Alarmfunktion lässt auf dem Smartphone für 20 Sekunden eine schrille Sirene ertönen. Das Gerät wird hierbei nicht gesperrt, somit dient die Funktion nur dem Wiederfinden eines verlegten Smartphones und nicht etwa der Abschreckung eines Diebs.

Gerät suchen

Diese Funktion ortet das das Gerät und zeichnet die Position in eine Google Maps Karte ein. Des Weiteren wird die Adresse angezeigt. Schön ist, dass die Positionen aller Geräte in eine gemeinsame Karte gezeichnet werden, sollte der Nutzer mehrere Geräte mit seinem Konto verknüpft haben. Die Ortung wird jeweils manuell gestartet, eine kontinuierliche Lokalisierung wird nicht angeboten.

Gerät sperren

Die Sperrfunktion blendet einen Sperrbildschirm ein, welcher Unbefugten den Zugriff auf das Handy verhindern soll. Der Nutzer kann im Webinterface einen vierstelligen, nummerischen PIN Code vergeben, welcher für die Entsperrung des Geräts notwendig ist. Alternativ kann die Entsperrung auch über das Webinterface durchgeführt werden. Sinnvoll ist, dass ein benutzerdefinierter Text auf dem Sperrbildschirm eingeblendet werden kann, welcher etwa einem ehrlichen Finder Informationen für die Rückgabe des Gerätes geben soll. Zusätzlich kann eine Telefonnummer angegeben werden, welche von einem Finder durch Tippen auf den Button „Eigentümer..." angerufen werden kann, ohne dabei die Nummer anzuzeigen.

Für die Entsperrung muss der zuvor definierte PIN Code eingegeben werden. Nach drei Fehlversuchen wird die PIN-Eingabe blockiert, es ist nur mehr über das Webinterface entsperrbar.

Die Sperrfunktion wurde insgesamt sehr solide ausgeführt. Es war uns nicht möglich die Sperre zu umgehen oder auf andere Art und Weise Zugriff auf das Gerät zu erlangen.

Daten von Gerät löschen

Diese Funktion ermöglicht das Löschen von Daten auf dem Gerät aus der Ferne. Der Nutzer kann im Webinterface entscheiden, welche Daten genau gelöscht werden sollen. Mit Hilfe von Checkboxen kann entschieden werden, ob nur Daten von der SD Karte oder der SIM Karte gelöscht werden sollen, sowie ob das Gerät auf Werkseinstellungen zurückgesetzt werden soll. Durch Rücksetzen auf Werkseinstellungen sind anschließend Funktionen wie die Lokalisierung nicht mehr verfügbar. Jedoch werden nur so alle Nutzerdaten wie Kontakte, SMS, Kalendereinträge, etc. gelöscht.

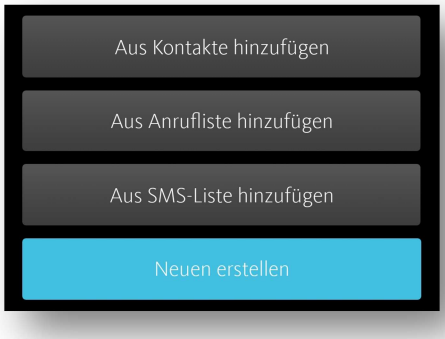
Auf unserem alternativen Gerät konnten wir auch das Löschen der Daten auf einer externen SD Karte testen. Auch diese Daten wurden wie erwartet gelöscht, konnten jedoch mit gängiger Freeware wiederhergestellt werden.

Identity Safeguard

Der Identity Safeguard warnt den Nutzer, wenn seine Emailadresse von großen Datenlecks betroffen ist. In der Vergangenheit war diesbezüglich zum Beispiel Adobe betroffen, wo eine große Anzahl an Datensätzen an die Öffentlichkeit gelangt ist. Avira prüft, ob die Emailadresse des Nutzers, oder eine Emailadresse eines Eintrags in der Kontaktliste, bei einem dieser großen Datenlecks an die Öffentlichkeit gelangt ist.

Blockierliste

Die Blockierliste ermöglicht das Blockieren von SMS und Anrufen von frei definierbaren Nummern. Der Nutzer kann die Nummer aus den Kontakten, der Anrufliste oder der SMS Liste importieren. Alternativ kann die Nummer auch manuell eingetragen werden. Für jeden Eintrag in der Blockierliste kann festgelegt werden, ob nur SMS, nur Anruf, oder beides blockiert werden soll.



Vor der ersten Verwendung der Funktion erscheint eine Meldung, dass es Probleme mit manchen LG Telefonen kommen kann, und dass die Blockierung von Telefonanrufen nicht funktionieren kann. Bei SMS soll es jedoch keine Probleme geben.

In unseren Tests trat das Gegenteil ein. Während Anrufe wie erwartet blockiert wurden, sind SMS durchgelassen worden. Auf diesen Zustand weist Avira jedoch in der Beschreibung im Google Play Store hin, da diese Funktion in der getesteten Android Version (4.4.2) nicht verfügbar ist. Auf einem alternativen Gerät hat auch das Blockieren der SMS funktioniert.

Upgrade

Avira bietet ein kostenpflichtiges Upgrade, welches zusätzlich zu den kostenlosen Funktionen eine „Secure Browsing“ Komponente hinzufügt. Diese schützt den Nutzer während des Browsens im Internet vor schadhaften Webseiten.

Updates

Updates werden automatisch durchgeführt. Dabei lässt sich das Intervall nicht einstellen. Bei der Gratisversion ist das Updateintervall einmal täglich, bei der kostenpflichtigen Variante stündlich. Manuelle Updates werden nicht unterstützt.

Hilfe

Avira bietet im Menü einen Hilfelink an, welcher auf *Avira Answers* verweist. Diese Seite ist jedoch mit dem Mobiltelefon nur schwer zu bedienen. Bei Avira Answers

handelt es sich um eine Community, welche häufige Fragen diskutiert.

Deinstallation

Vor der Deinstallation muss Avira aus der Liste der Geräteadministratoren ausgetragen werden. Hierfür bietet Avira einen Assistenten an, welcher alle notwendigen Schritte einleitet. Abschließend wird der Nutzer nach dem Grund der Deinstallation befragt, was jedoch übersprungen werden kann.
Für die Deinstallation ist kein Kennwort notwendig. Ein Dieb kann somit die Diebstahlschutzfunktion deinstallieren, sofern der Bestohlene noch keine Fernsperrung durchgeführt hat.

Lizenz

Avira Antivirus Security ist im Google Play Store frei verfügbar. Für die Zusatzfunktionen Sicheres Browsing, stündliche Updates sowie erweiterter Support sind 7,95€ jährlich zu bezahlen.

Fazit

Avira bietet mit Avira Antivirus Security ein sehr schön gestaltetes Sicherheitsprodukt für Android Smartphones. Der Diebstahlschutz lässt sich über ein ebenso schickes Webinterface steuern. Innovative Funktionen wie der Identity Safeguard runden das Produkt ab. Avira scheint auf Qualität statt Quantität zu setzen. Auch wenn der Funktionsumfang im Vergleich zu anderen Produkten gering ist wurden die vorhandenen Komponenten vernünftig ausgeführt. Wünschenswert wäre jedoch ein Passwortschutz für die Deinstallation des Sicherheitsprodukts.

Baidu Mobile Security

Baidu Mobile Security ist ein Sicherheitsprodukt für Android, welches kostenlos zur Verfügung gestellt wird und einen großen Funktionsumfang bietet. Dazu gehört eine Tuning-Funktion, App Manager, Schutz vor Störanrufen, Antivirus und Schutz bei mobilen Bezahlvorgängen.

Installation

Wir haben Baidu Mobile Security von der offiziellen Seite des Herstellers geladen. Die Installation war simpel und problemlos.

Starten des Programms

Beim ersten Starten des Programms wird der Schutz während dem mobilen Bezahlen beworben.

Sowohl das Akzeptieren der Lizenzvereinbarung, sowie das Senden von Feedback sind standardmäßig aktiviert. Der Nutzer kann entweder den Schutz bei mobilen Bezahlvorgängen testen oder durch Antippen des entsprechenden Buttons in der rechten oberen Ecke zum Starbildschirm wechseln.

Vom Startbildschirm aus, können alle Funktionen durch einfaches Tippen erreicht werden.

Health Checkup

In der Mitte des Bildschirms wird der aktuelle „Health" Status eingeblendet. Die Checkup-Funktion kann Speicher freigeben, beendet laufende Prozesse und löscht Trash-Files. Die Funktion empfiehlt zudem die Aktivierung der „Sicher Bezahlen" Funktion, sowie die Aktualisierung von bereits installierten Applikationen. Außerdem wird darauf aufmerksam gemacht, dass noch kein Systemscan durchgeführt wurde. Letztgenannter hat in unserem Test eine App, welche von Aochan Supermarktkette vertrieben wird, als schadhaft klassifiziert.

Während des Checkups wird zudem die Installation des Baidu Appstores empfohlen, welcher „sichere App Downloads" garantieren soll.

Mobile Speedup

Nach dem Durchführen des Checkups findet Baidu noch weitere Möglichkeiten das Gerät zu optimieren. Laut Anwendung wurden 500

MB an Speicher durch den „Smart Speedup“ freigegeben.
Die Komponente bietet zudem einen „Deep Speedup“, welcher zuerst installierte Apps auf dem Gerät über einen längeren Zeitraum analysiert. Apps können jedoch nicht angehalten werden oder der CPU Takt geändert werden, ohne das Gerät zu rooten.

Trash removal

Nach dem ersten Check-up und dem Speed-up fand die Trash-Removal Funktion immer noch 45 MB an Daten auf unserem Testgerät. Die „Deep Removal Funktion“ hat sogar 92,5 MB an angeblich nicht mehr benötigten Dateien gefunden und gelöscht.

Mobile fee protection & data volume monitor

Die aktuelle Version der Baidu Applikation bietet eine Menge an Funktionen um den Nutzer vor zu hohen Telefonrechnungen zu schützen. Auf der Registerkarte „Protection against waste of mobile fees“ kann der Nutzer das verfügbare Guthaben sowie das bereits verwendete Downloadvolumen einsehen. Zudem kann ein Scan nach Applikationen gestartet werden, welche speziell nach Apps sucht, die hohe Telefonrechnungen verursachen können. Zudem kann eingesehen werden welche Apps ungewöhnlichen Datenverkehr erzeugen, Mehrwertdienste können gekündigt und das SMS Postfach nach betrügerischen Nachrichten gescannt werden.
Auf unserem Testgerät mit einer China Unicom Prepaid SIM Karte hat die Überprüfung von Mehrwertdiensten nicht funktioniert. Eine Einblendung hat uns darüber informiert, dass Unicom-Nutzer Kontakt zum Mobilfunkbetreiber aufnehmen sollen, um aktvierte Mehrwert-Abos zu überprüfen.

Data Traffic Monitor

Diese Komponente überwacht den Datenverkehr des Nutzers. Zudem kann sich die Applikation Daten mit mobilen Bezahlsystemen des Mobilfunkproviders synchronisieren und Daten austauschen. Außerdem können zusätzliche Volumina für die Mobilfunknutzung bestellt werden. Zudem wird der Nutzer benachrichtigt, wenn er etwa Roamingdienste in Anspruch nimmt, welche

nicht durch seinen Mobilfunkvertrag abgedeckt sind.

Distrubance blocker

Spam SMS und Störanrufe sind nach wie vor ein großes Problem in China. In unserem Test hat die Applikation erfolgreich Spam SMS geblockt. Bedauerlicherweise wurde keine der Telefonnummern von Werbeanrufen geblockt, die während des Testzeitraumes eingegangen sind.

Security Tools

Unter diesem Reiter kann eine große Anzahl an Sicherheits- (sowie Nicht-Sicherheits-) Tools heruntergeladen und installiert werden. In unserem Test wurde eine Taschenlampenapp, WiFi Radar, Energiesparapplikationen, one-click Root, Speedup Apps und weitere angezeigt.

Secure Payment

Dieser Komponente wurde eine eigene Tab-Seite gewidmet. Hier werden Links zu den offiziellen Bankingapps bereitgestellt. Applikationen wie die Kuaidi Taxi App und die Software „Alipay wallet“ können in einem „Sicheren Umfeld“ ausgeführt werden. Zudem kann die Seriosität und Sicherheit des aktuell verbundenen WLAN Netzwerkes überprüft werden. Als letzte Schutzfunktion wird der Schutz von Textnachrichten, welche von Online Bezahldiensten stammen, geboten.

Weitere Funktionen

In der unteren Ecke des Startbildschirmes kann der Nutzer den AV-Scanner finden, gleich neben einer Funktion, die das Rooten des Geräts ermöglicht, einem weiteren Speicherbereinigungstool, einem App Uninstaller, einem Adware Scanner, einem Privacy Scanner und einer sichere Eingabemaske für die Suchmaschine von Baidu.

Der Adware Scanner hat in unserem Test ein Problem betreffend die Privatsphäre in der Applikation „Amazing Alex“ gefunden, da sie die Nummer des Geräts auslesen kann. Baidu hat empfohlen die App zu deinstallieren.

AV Scanner

Baidu bietet zwei Varianten von Scans, einen „Complete Scan“, sowie einen „Quick Scan“. Die Malwaredefinitionen werden automatisch aktualisiert. Eine Cloudscan-Funktion ist standardmäßig aktiviert, zudem werden Apps bereits während der Installation gescannt.

Die Aochan App, welche vom Baidu Adware Scanner als sauber eingestuft wurde, wurde vom AV-Scanner als schadhaft eingestuft. Baidu empfahl die sofortige Deinstallation.

The Baidu Spaceship

Seit der Installation der Baidu App wird ein kleiner Kreis auf dem Desktop des Geräts angezeigt. Durch Ziehen dieses Kreises in die Mitte des Bildschirms, welche die Einblendung eines animierten Raumschiffs bewirkt, wird ein Quick Cleanup durchgeführt.

Deinstallation

Es wird kein Deinstallationsassistent angeboten. Des Weiteren ist kein Passwort für die Deinstallation notwendig. Da keine Diebstahlsicherung vorhanden ist halten wir dies auch nicht für notwendig.

Lizenz

Baidu Mobile Manager wird kostenlos zur Verfügung gestellt.

Fazit

Baidu Mobile Security ist ein einfach zu verwendendes Produkt, welches wichtige Funktionen wie einen Blocker von Störanrufen, welcher jedoch verbessert werden könnte, und sicheres Bezahlen bietet.

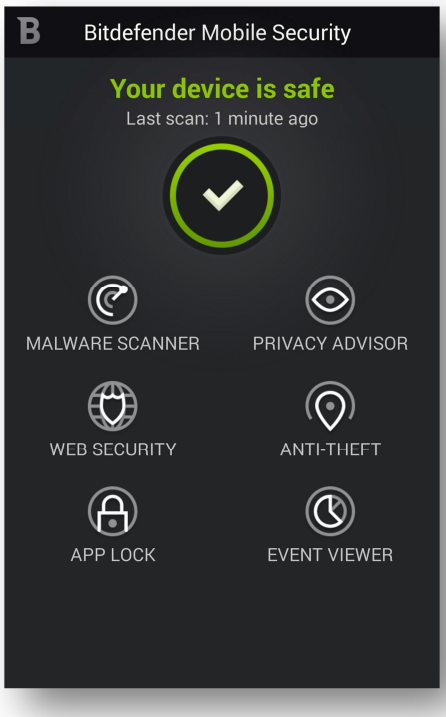
Außerdem wird der Nutzer nicht offensiv genug auf mögliche Gefahren hingewiesen. Nutzer mit wenig technischem Verständnis könnten fälschlicher Weise anhand der Health Score vermuten, dass alles in Ordnung sei und dass keine weiteren Überprüfungen notwendig seien, wie in folgender Tabelle veranschaulicht wird:

Health score	92
Ad scanner	No risk
Av scanner	VIRUS

Zudem halten wir es nach wie vor wichtig einen Diebstahlschutz zu integrieren, welcher nicht implementiert wurde. Der unbefugte Zugriff auf private Daten von Unbefugten, etwa bei einem Diebstahl sollte nicht unterbewertet und entsprechend berücksichtigt werden.

Bitdefender Mobile Security

Bitdefender Mobile Security ist als 14-tägige Testversion verfügbar. Nach Ablauf dieses Zeitraums muss der Nutzer eine Lizenz erwerben um die Software weiter verwenden zu können. Bitdefender vereint mit seinem Produkt einen Cloud basierten Malware Scanner mit einem Surf- und Diebstahlschutz. Über SMS, sowie ein Webinterface können die Anti-Theft Funktionen gesteuert werden, welche das Lokalisieren, Sperren und Löschen des Geräts ermöglicht. In der aktuellsten Version ist zudem eine Erweiterung für Android Wear integriert, welche Nutzern das Steuern der Diebstahlschutzfunktion mit der Smartwatch ermöglicht.

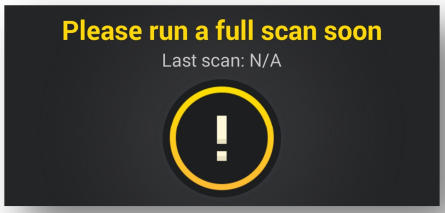


Installation

Bitdefender wurde aus dem Google Play Store kostenlos bezogen und installiert. Als erster Schritt müssen die Lizenzvereinbarungen akzeptiert werden. Zusätzlich kann der Nutzer einstellen, ob er anonyme Statistiken an Bitdefender übertragen möchte (Opt-Out).
Anschließend muss dem Gerät ein Name gegeben werden, um es im Webinterface identifizieren zu können. Anschließend muss das Gerät mit einem Benutzerkonto verknüpft werden. Hierfür kann entweder ein Konto angelegt werden, oder praktischerweise auch einfach das Google Konto verwendet werden. Abschließend muss das Produkt lizensiert werden. Es kann entweder eine 14-tägige Testversion gestartet, eine Lizenz erworben, oder ein bestehender Produktschlüssel eingegeben werden.

Starten des Programms

Nach erfolgreicher Installation wird der Nutzer auf den Homescreen weitergeleitet. Hier sticht sofort die gelbe Aufforderung zum baldigen Ausführen eines Malwarescans, sowie ein oranger Banner, der auf die 14-tägige Testversion aufmerksam macht, ins Auge.
Nach einem durchgeführten Malwarescan erscheint als Status einer der drei Möglichkeiten: grün signalisiert, dass kein Sicherheitsrisiko besteht, oder gelb oder rot, die darauf aufmerksam machen, dass Sicherheitsrisiken bestehen und eventuell der User aktiv werden muss.



Über den Updatestatus berichtet Bitdefender nichts. Dies liegt daran, dass lokal keine Virendefinitionen gespeichert sind, sondern eine direkte Anbindung zur Bitdefender Cloud besteht.

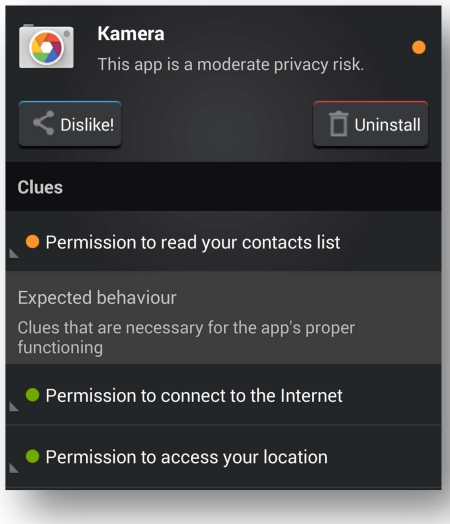
Malware Scanner

Der Virenscanner bietet dem Anwender die Möglichkeit, die installierten Apps und den Speicher des Mobiltelefons auf Malware zu überprüfen. Die Überprüfung des Speichers ist hierbei optional, die installierten Apps werden bei jedem Durchlauf gescannt. Diese werden auch automatisch während der Installation gescannt.

Der Malware Scanner funktioniert nur mit bestehender Internetverbindung, da die Cloud für die Erkennung herangezogen wird.

Privacy Advisor

Der Privacy Advisor analysiert installierte Apps ob sie die Möglichkeit haben private Informationen des Nutzers aufzuzeichnen und so die Privatsphäre des Nutzers ohne sein Wissen zu verletzen. Um den Nutzer nicht mit Details zu überfluten gibt Bitdefender eine Punktezahl zwischen 0 und 100 an, um die gesamte Sicherheitssituation zu bewerten. Je niedriger die Zahl ist, umso mehr Apps mit fragwürdigen Berechtigungen wurden erkannt. Des Weiteren werden alle installierten Applikationen aufgelistet. Durch Antippen eines Eintrags werden alle Berechtigungen detailliert aufgeschlüsselt.



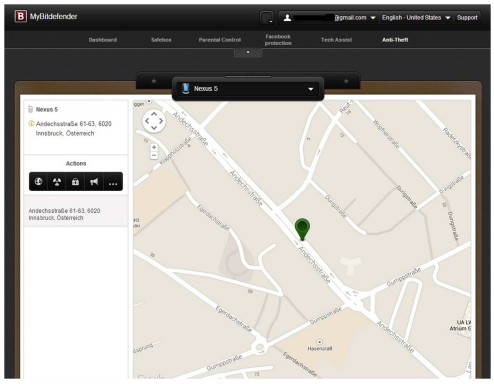
Dies wurde unserer Meinung nach auch gut umgesetzt. So werden die Berechtigungen in „Erwartetes Verhalten“ und „Clues“ eingeteilt. Somit können auch unerfahrenere Anwender die Informationen einordnen und abschätzen ob die Applikation wohl ausspioniert oder nicht. In der Ansicht kann die Applikation anschließend direkt deinstalliert werden.

Web Security

Web Security schützt den Nutzer während dem Surfen im Internet vor gängigen schadhaften Angriffen. Bitdefender gibt an vor Phishing, Betrug und Malware zu Schützen.

Anti-Theft

Der Diebstahlschutz von Bitdefender kann entweder über ein schönes Webinterface (http://my.bitdefender.com), oder über SMS Kommandos gesteuert werden. Er ist standardmäßig deaktiviert, kann jedoch schnell aktiv geschalten werden. Dazu muss die Applikation als Geräteadministrator eingetragen werden um ihr ausreichend Privilegien für die Durchführung von Lösch- und Sperrkommandos zu verleihen. Bitdefender gibt gleich den Hinweis, dass vor der Deinstallation der Applikation die Geräteadministratorberechtigung deaktiviert werden muss. Um den Vorgang abzuschließen muss ein vier- bis achtstelliger PIN vergeben werden (nummerisch). Zusätzlich muss ein vertrauenswürdiger Freund eingetragen werden. Dieser wird benachrichtigt wenn die SIM Karte gewechselt wird, und ist die einzige Nummer von der das Wipe-Kommando akzeptiert wird.



Locate

SMS Kommando: BD-<PIN> LOCATE

Die Locate Funktion lokalisiert ein verlorengegangenes oder gestohlenes Gerät. Im Webinterface wird die Position in eine Karte von Google Maps eingetragen. Die Möglichkeit einer kontinuierlichen Ortung zum Aufzeichnen des Bewegungsprofils besteht nicht.

Bei Verwendung von SMS Kommandos wird an den Absender eine Antwort mit einem Link auf eine Karte von Google Maps gesendet.

Scream

SMS Kommando: BD-<PIN> SCREAM

Die Scream Funktion lässt auf dem Gerät eine schrille Sirene ertönen. Dabei wird es nicht gesperrt. Somit handelt es sich hierbei mehr um eine Funktion um ein verlegtes Gerät in der Wohnung wiederzufinden und nicht um zum Beispiel einen Dieb abzuschrecken.

Lock

SMS Kommando: BD-<PIN> LOCK

Dieser Befehl sperrt das Gerät und schützt somit vor unbefugtem Zugriff. Dabei setzt Bitdefender auf den in Android integrierten Sperrbildschirm. Dieser ermöglicht zwar nicht das platzieren von Nachrichten oder Logos, dafür gibt es keinerlei Beanstandungen bezüglich der Sicherheit. Es ist nicht möglich ihn zu umgehen, außerdem kann jederzeit ein Notruf abgesetzt werden.

Wird der Befehl mittels SMS abgesetzt, so kann das Gerät mit dem zuvor angegebenen Anti-Theft PIN entsperrt werden. Über das Webinterface kann ein vierstelliger PIN frei vergeben werden.

Wipe

SMS Kommando: BD-<PIN> WIPE

Dieses Kommando setzt das Gerät auf Werkseinstellungen zurück und löscht somit alle darauf befindlichen Daten. Sollte der Befehl per SMS abgesetzt werden, so wird dieser nur von der vertrauenswürdigen Person, welche zuvor eingetragen wurde, akzeptiert.

In unserem Test hat diese Komponente gut funktioniert, jedoch wurden von der externen SD-Karte wie schon im Vorjahr, keine Dateien gelöscht.

Callme

SMS Kommando: BD-<PIN> CALLME

Diese Funktion kann nur mithilfe von SMS Kommandos ausgeführt werden. Nach Absetzen des Kommandos wird der Absender des SMS angerufen und der Lautsprecher des Smartphones aktiviert. Somit ist es einem Bestohlenen möglich zum Beispiel möglich Kontakt mit einem ehrlichen Finder aufzunehmen um etwa eine Rückgabe zu vereinbaren.

Help

SMS Kommando: BD-<PIN> HELP

Ein unterschätztes aber durchaus wichtiges Kommando ist der Help-Befehl. Er sendet an den Absender der SMS eine Liste mit allen verfügbaren Befehlen. Dies kann durchaus Sinn machen, denn im Falle eines Verlusts kann sich der Nutzer nicht an die verfügbaren Befehle erinnern.

SIM Change

Wenn die SIM Karte des Smartphones ausgetauscht wird, zum Beispiel dann, wenn ein Dieb seine eigene einsteckt, wird ein SMS an die zuvor eingetragene Vertrauensperson gesendet. Diese Person soll dann bei der Wiederfindung des gestohlenen Geräts behilflich sein.

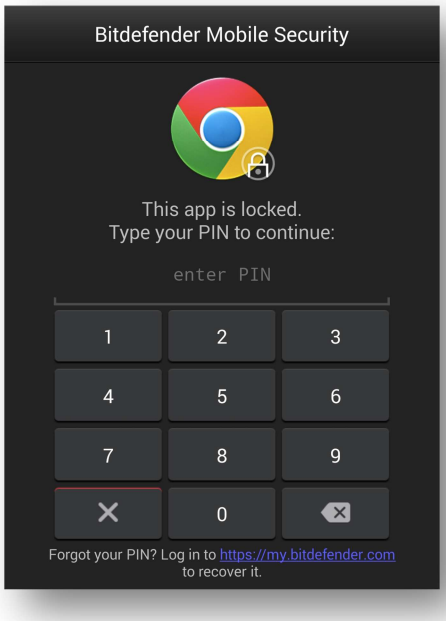
Diese Funktion hat in unseren Tests nicht funktioniert. Wir haben das Szenario genau nachgespielt – es wurde kein SMS versandt, auch andere Aktionen des Sicherheitsprodukts konnten nicht festgestellt werden. Auf dem alternativen Testgerät mit Android 4.1.2 hat die Funktion jedoch einwandfrei funktioniert.

Upload Location

Diese Funktion sendet die Koordinaten des Geräts bevor die Batterie des Geräts leer ist. So kann der Nutzer sein Gerät möglicherweise wiederfinden, selbst wenn der Akku erschöpft ist.

App-Lock

App-lock ist eine Funktion, welche neu in Bitdefender hinzugefügt wurde. Diese ermöglicht einen Passwortschutz von installierten Apps. Der Nutzer kann einstellen, für welche Apps ein Passwort notwendig sein soll. So kann etwa eingestellt werden, dass für das Öffnen der Galerie ein PIN eingegeben werden muss. Dies kann zum Beispiel hilfreich sein um Kindern den Zugriff zu gewissen Funktionen zu verhindern.



Updates

Da Bitdefender keinen offline Malwarescan anbietet, sondern stets die Bitdefender Cloud für die Überprüfung von Dateien verwendet sind Updates obsolet.

Hilfe

Bitdefender bietet dem Nutzer am Smartphone keine explizite Hilfe an. Für jede Funktion existiert allerdings eine kurze, jedoch nützliche Kurzinformation.

Deinstallation

Für die Deinstallation wird dem Nutzer kein Assistent angeboten. Hierfür ist eine PIN Eingabe notwendig, das Dieben das Entfernen der Diebstahlsicherung unmöglich machen soll.

Lizenz

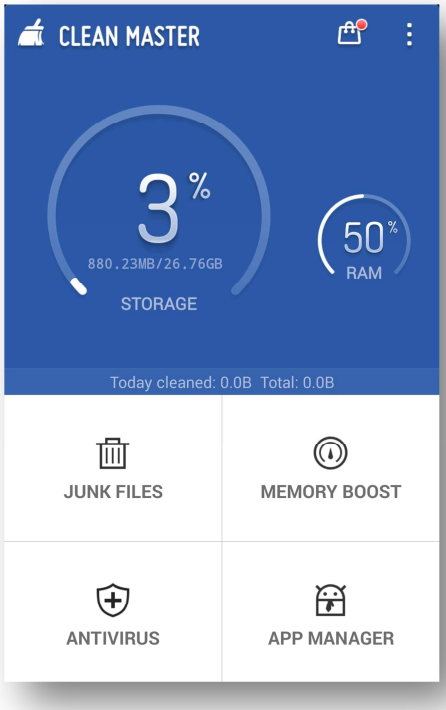
Bitdefender Mobile Security PREMIUM kann für 14 Tage kostenlos getestet werden. Danach ist eine Lizenz erforderlich, die für 9,95€ pro Jahr oder 0,99€ pro Monat per In-App-Kauf erhältlich ist.

Fazit

Bitdefender Mobile Security wurde im Vergleich zum letzten Jahr optisch überarbeitet und mit einem App Blocker ausgestattet. Die Funktionen sind durchdacht und haben im Allgemeinen sehr gut funktioniert. Lediglich beim Wechseln der SIM Karte wurden in unseren Tests keine SMS an die Vertrauensperson gesendet.

CheetahMobile Clean Master

CheetahMobile Clean Master bietet dem Nutzer ein Sicherheitsprodukt, welches auf die Säuberung des Telefons ausgerichtet ist. So stehen Antivirus, Junk Entfernung und Memory Boost zur Verfügung. Auf einen Diebstahlschutz wird jedoch verzichtet.



Installation

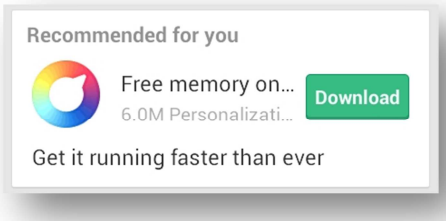
CheetahMobile Clean Master wurde aus dem Google Play Store bezogen und installiert. Die Installation erforderte keine weitere Konfiguration. Der Nutzer wird auf den Startbildschirm weitergeleitet.

Starten des Programms

Beim Starten des Programms wird auf dem Startbildschirm der aktuelle Speicherverbrauch (Datenspeicher), sowie der aktuelle RAM Verbrauch angezeigt. Außerdem werden Statistiken angezeigt wie viele Byte heute bereits bereinigt wurden. Da das Programm frisch installiert wurde stehen die beiden Anzeigen noch auch 0 Byte. Durch Antippen des Speicher- und RAM Symbols werden detaillierte Auflistungen des Speicherverbrauchs aufgelistet.

Junk Files

Diese Funktion findet nicht benötigte Dateien, wie zum Beispiel Cache Dateien, im lokalen Dateisystem. Dem Nutzer wird angeboten diese Dateien zu löschen und das System so zu bereinigen. Unser Gerät, welches bis jetzt nur für ein paar wenige Tests verwendet wurde, wies laut Clean Master bereits einen Umfang von 578MB Junkfiles auf. Unter den zu löschenden Daten befanden sich obsolete APK Dateien, nicht mehr benötigte Daten im Telefonspeicher, sowie Dateien die im Cache liegen. Nach dem Abschluss der Aktion wird das Ergebnis eingeblendet (575MB bereinigt), sowie Empfehlungen zur Installation weiterer Produkte von CM angezeigt.

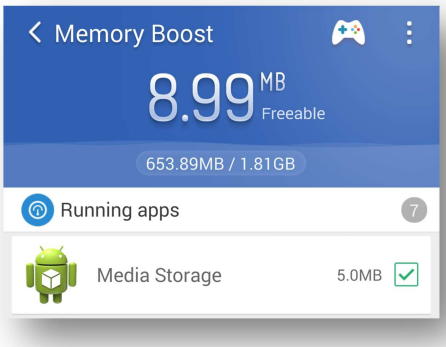


Nach kurzer Verwendung des Geräts (ohne andere Anwendungen zu starten) konnten abermals 177MB Speicher bereinigt werden. Cheetah hat uns darüber in Kenntnis gesetzt, dass dies auf Hintergrunddienste zurückzuführen ist, welche stetig Junkdateien erzeugen.

Es ist möglich das Löschen von Junk Files automatisch ausführen zu lassen. Hierfür stehen dem Nutzer Intervalle von täglich bis 15-täglich zur Verfügung. Außerdem ist es möglich nach Dateitypen zu Filtern. So kann zum Beispiel festgelegt werden, dass JPG Dateien von der Bereinigung ausgeschlossen sind.

Memory Boost

Die Memory Boost Funktion bereinigt den RAM von überflüssigen Daten laufender Applikationen.

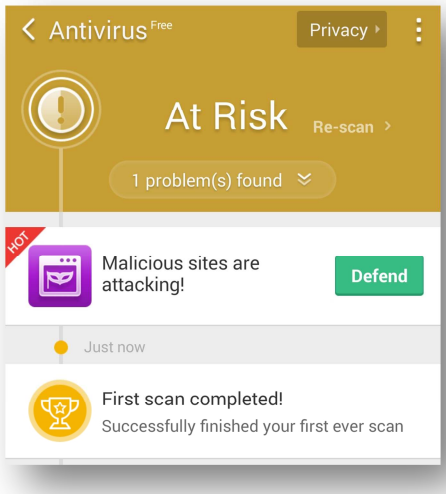


In unserem Test wurden etwa Apps wie die Uhr oder Media Storage angezeigt. Zusätzlich werden Apps wie Hangouts angezeigt, wofür jedoch eine Empfehlung gegeben wird die Daten im RAM zu belassen. In unserem Test konnten 9MB an Daten aus dem RAM entfernt werden.

Antivirus

Die Antiviruskomponente des Produkts untersucht das Gerät nach möglichen Problemen, die die Sicherheit betreffen können. Die bloße Überprüfung des Dateisystems nach Malware ist für CheetahMobile jedoch nicht genug. So wird in unserem Test zum Beispiel angezeigt, dass ein Browserverlauf erstellt wurde (Chrome), welche gelöscht werden könnte. Des Weiteren ist ein Echtzeitschutz vorhanden.

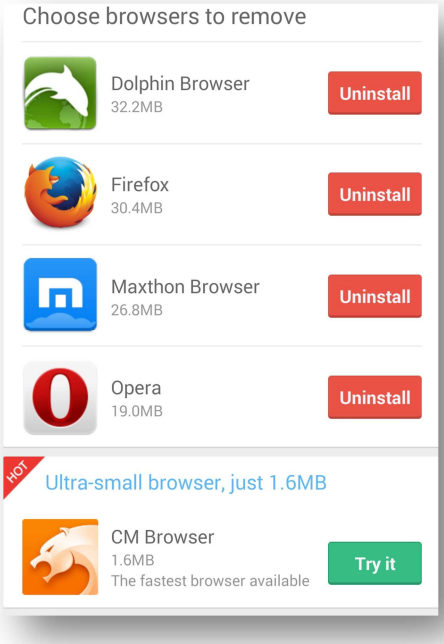
In der oberen Ecke des Bildschirms wird ein Button mit der Aufschrift „Privacy“ angezeigt. Mit diesem kann der Nutzer Daten löschen, welche Informationen über das Nutzungsverhalten des Geräts aussagen könnten. Hierzu gehört zum Beispiel der Suchverlauf im Google Play Store. Durch einfaches Klicken auf „Clean“ können derartige Einträge vom Gerät entfernt werden. Zusätzlich zu den Daten, die automatisch gelöscht werden können, besteht auch die Möglichkeit der manuellen Säuberung. Hierfür leitet Clean Master zu den jeweiligen Einstellungen der Apps weiter, wo dann der Cache und andere Daten gelöscht werden können.



Nach dem Durchführen des Virenscans wird eine Meldung eingeblendet, dass „Gefährliche Seiten attackieren“ und man diese Gefahr abwehren müsse. Hinter dem „Defend“-Button verbirgt sich jedoch abermals nur eine Weiterleitung auf den Google Play Store, um den eigenen CM Browser an den Mann zu bringen. Diese Wortwahl halten wir für übertriebene Panikmache, stattdessen sollte neutral auf den sicheren Browser hingewiesen werden. Wir haben den Test auf mehreren Geräten wiederholt, haben dieselbe Benachrichtigung jedoch nicht reproduzieren können, da stets unterschiedliche Benachrichtigungen eingeblendet werden.

App Manager

Im Appmanager werden installierte Anwendungen aufgelistet. So wird etwa angezeigt, dass vier Browser installiert sind, die zusammen 108MB Speicherplatz verwenden. Diese können dann direkt aus diesem Menü deinstalliert werden. Gespart wird hierbei auch nicht an der Platzierung von Anzeigen für den hauseigenen CM Browser. So wird vorgeschlagen die installierten Browser (Opera, Dolphin, Maxthon und Firefox) zu deinstallieren und durch den eigenen CM Browser zu ersetzen.



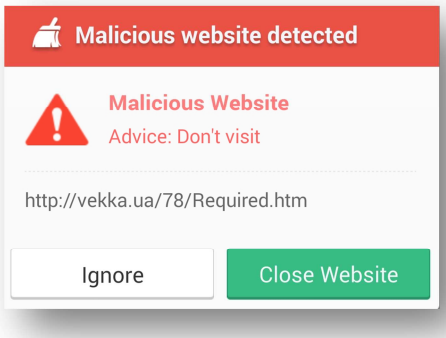
Am Ende der Liste der installierten Apps werden anschließend weitere, empfohlene Apps angezeigt (rund 100). Durch Wischen nach rechts wechselt das Userinterface zu den „Picks“, einem Appstore wo besonders beliebte Apps gelistet werden.

In einer weiteren Tabpage werden APK Dateien gelistet, welche im Dateisystem gefunden wurden. Hierbei steht jedoch die Entfernung der Datei im Vordergrund, auch wenn es möglich ist in der Detailansicht die APK Datei auszuführen und somit zu installieren.

Eine weitere Funktion des Appmanagers ist es, Daten von Apps vom internen Speicher auf den externen zu verschieben. Dies kann sinnvoll sein, wenn der interne Speicher sehr begrenzt ist, jedoch eine große SD Karte im Gerät verfügbar ist. Die Funktion war jedoch mit unseren beiden Testgeräten nicht kompatibel.

Safe Browsing

Clean Master hat eine Safe Browsing Funktion integriert. So kann das Produkt während dem Surfen im Internet vor betrügerischen und gefährlichen Seiten warnen und den Nutzer schützen.



Die Funktion hat in unserem Kurztest ohne Probleme funktioniert.

Updates

Wir konnten keine Informationen bezüglich Updates finden. Ein Klick auf den Update-Button leitet uns auf den Google Play Store weiter.

Hilfe

Es werden FAQ angeboten, welche einen Umfang von 42 haben. Zwar werden dadurch einige Unklarheiten abgedeckt, jedoch wäre eine konventionelle Hilfe trotzdem hilfreicher.

Deinstallation

Die Deinstallation des AV-Produkts kann über den androidinternen Appmanager durchgeführt werden. Hierfür ist keine Passworteingabe notwendig. Dies ist auch in Ordnung so, da kein Diebstahlschutz geboten wird.

Lizenz

CheetahMobile Clean Master ist kostenlos in vollem Funktionsumfang verfügbar.

Fazit

CheetahMobile geht mit Clean Master einen anderen Weg wie die meisten anderen Sicherheitsprodukte im Test. Auf Diebstahlschutz wurde verzichtet, stattdessen der Fokus auf Säuberung des Geräts gelegt. Die Cleanup-Funktionen haben in unseren Tests angeblich erstaunliche Mengen an Speicher freigeben können.

In unseren Augen ist besonders bei mobilen Geräten die Gefahr von Verlust oder Diebstahl

allgegenwärtig. Auch wenn die Antivirus und Cleanup Komponenten gut funktionieren, würde ein Diebstahlschutz das AV-Produkt abrunden. Nutzer sollten sich in Acht nehmen, dass Cheetah Clean Master dazu rät andere (gute) Software zu deinstallieren, um sie durch eigene Produkte zu ersetzen.

CheetahMobile CM Security

CM Security ist kostenlos verfügbar und bietet sinnvolle Funktionen wie Antivirus und Diebstahlschutz. Um störende Anrufer abzuweisen kann der integrierte Callfilter eingesetzt werden.

Installation

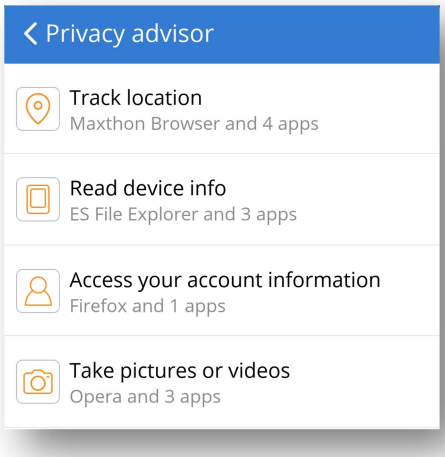
CM Security wurde aus dem Google Play Store bezogen und installiert. Die Installation war problemlos und erforderte keine weiteren Nutzeraktionen.

Starten des Programms

Beim ersten Start des Programms erscheinen ein gelber Status und der Hinweis, dass noch kein Security Scan durchgeführt wurde. Nach der Durchführung warnt CheetahMobile, dass *Safe browsing* noch nicht aktiviert wurde. Nach der Aktivierung wechselt der Status auf blau und die Meldung „System is protected“ wird angezeigt.

Antivirus

Ein Antivirenscan kann direkt vom Startbildschirm aus gestartet werden. Dieser scannt nur die installierten Apps und das System. Um auch die SD-Karte und den integrierten Speicher zu überprüfen, kann im Kontextmenü „Scan SD Card“ gewählt werden. Nach Abschluss des Scans werden die Resultate gelistet. Hier macht CheetahMobile darauf aufmerksam *Safe Browsing* zu installieren. Hierbei handelt es sich lediglich um eine Weiterleitung auf den hauseigenen „CM Browser“ im Google Play Store.



Des Weiteren findet man in den Ergebnissen einen Privacy Advisor. Dieser listet in vier Kategorien mögliche Verletzungen der Privatsphäre. In unserem Test wurden „Ortung“, „Device Info“, „Access Account Information“ und „Erstellen von Fotos und Videos“ angeführt. Durch Antippen einer der Kategorien werden die jeweiligen Applikationen aufgelistet, welche die entsprechenden Berechtigungen besitzen. Tippt der Nutzer eines der gelisteten Apps an, so werden Details angezeigt. Diese sind in unseren Augen jedoch ein wenig optimierungsbedürftig. So wird jeweils immer nur die Berechtigung der jeweiligen Kategorie aufgelistet. Ist ein App jedoch in mehreren Kategorien vertreten, so muss der Nutzer in jeder der Kategorien suchen und kann mangels Übersicht nur schwer entscheiden ob das App tatsächlich die Privatsphäre verletzen kann, oder nicht.

Anschließend kann der Nutzer eine Bewertung abgeben, indem er „Vertrauen“ oder „Fraglich“ anklickt. Diese Bewertung wird offenbar an CheetahMobile übertragen.

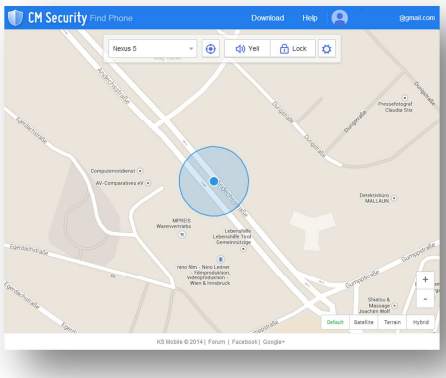
Zusätzlich zeigt CM Security an, dass Echtzeitschutz, Safe Browsing und automatische Updates aktiviert sind.
Die SD Karte, sowie der integrierte Speicher kann über einen entsprechenden Eintrag im Kontextmenü gescannt werden.
In den Einstellungen können automatische Scans eingestellt werden. So ist es etwa möglich täglich, wöchentlich oder monatlich automatisch durchführen zu lassen.

Clean Up Junk

Beim ersten Start dieser Komponente werden wir aufgefordert diese Komponente nachzuinstallieren. Nach dem Fortsetzen wird der Nutzer auf den Google Play Store weitergeleitet, zur Applikation „Clean Master" von CheetahMobile (Siehe auch CheetahMobile Clean Master - Insofern werden wir die detaillierte Beschreibung hier überspringen).

Find Phone

Unter diesem Menüpunkt findet der Nutzer den Diebstahlschutz. Bei der erstmaligen Einrichtung muss das Gerät einem Nutzerkonto hinzugefügt werden. Hierfür muss ein Google Konto angegeben werden. Anschließend muss ein Entsperrmuster festgelegt werden, welches für die Bildschirmsperre verwendet wird. Hierfür müssen mindestens vier Punkte verbunden werden.



Locate

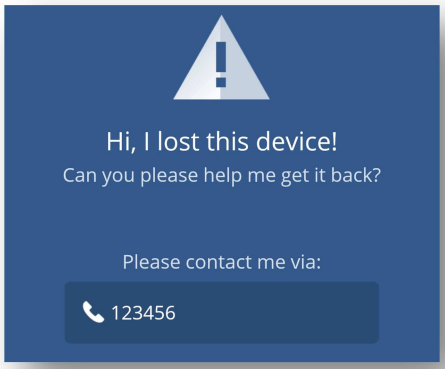
Diese Funktion lokalisiert das Gerät und zeigt die Position in einer Google Maps Karte an. Beim ersten Öffnen des Webinterfaces wird das Gerät automatisch geortet.

Yell

Dieses Kommando lässt auf dem Gerät für 60 Sekunden eine schrille Sirene ertönen. Dabei wird es nicht gesperrt. Dies kann zum Beispiel hilfreich sein um ein verlegtes Gerät wiederzufinden.

Lock

Mit dem Lock Befehl wird das Gerät mit dem zuvor festgelegten Sperrmuster gesperrt. Dies ist insgesamt sehr solide ausgeführt, wir konnten die Sperre nicht umgehen. Zusätzlich fanden wir es sehr gut, dass wir sowohl Telefonnummer, als auch Emailadresse angeben können, die es einem ehrlichen Finder erleichtern sollen ein gestohlenes Gerät zurückzugeben.



Makellos ist der Sperrbildschirm jedoch nicht. So kann kein Notruf mehr abgesetzt werden, was im Notfall sehr problematisch sein kann. Zum anderen war es möglich das Android Notification Center zu öffnen, wo es möglich ist das Gerät in den Flugzeugmodus zu versetzen. Anschließend ist der Diebstahlschutz weder für Webinterface, noch für SMS verfügbar und ist somit komplett deaktiviert.
Gut gelöst war, dass nach mehrmaliger Falscheingabe der Bildschirm für eine Minute gesperrt ist. Dies erschwert Brute-Force Attacken.

Wipe

Die Wipefunktion löscht persönliche Daten vom Gerät des Nutzers um sie für dritte unzugänglich zu machen.

In unseren ersten Tests konnten wir die Wipefunktion nicht testen, da ein entsprechender Button im Webinterface nicht eingeblendet war. Nach Kontaktaufnahme mit dem Hersteller hat uns dieser mitgeteilt, dass die Wipefunktion in unserer Region (Österreich) nicht verfügbar sei (In der App wurde jedoch „Enabled“ angezeigt!). Letztendlich hat CheetahMobile die Funktion auch für unsere Region aktiviert worauf wir den Wipe unter die Lupe genommen haben.

Die Funktion setzt das Gerät nicht auf Werkseinstellungen zurück. Dies hat den Vorteil, dass der Diebstahlschutz weiterhin aktiv bleibt und das Gerät weiterhin geortet werden kann. CheetahMobile hat jedoch auf das Löschen einiger persönlicher Daten vergessen. So war es weiterhin möglich auf die Mails, Kalendereinträge, den Browserverlauf und die Bookmarks zuzugreifen. Außerdem wurden auf dem Nexus die SMS nicht gelöscht, worauf der Hersteller auch im Webinterface aufmerksam macht. Einschränkungen in der Androidversion (4.4) wird hierfür als Grund genannt. Auf dem Samsung Galaxy mit Android 4.1.2 wurden die SMS Nachrichten gelöscht.

Auf unserem alternativen Testgerät wurde die externe SD Karte wie erwartet gelöscht. Es war uns jedoch ein Leichtes die gelöschten Dateien mit Freewaretools wiederherzustellen.

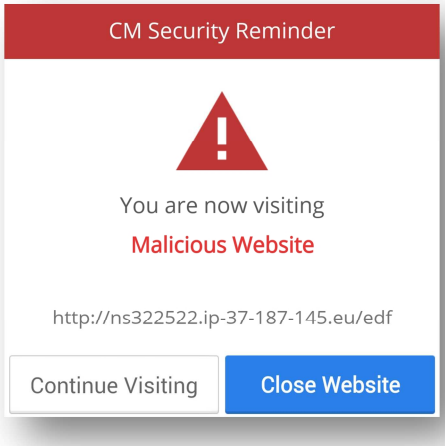
Beim Wipe sehen wir also noch durchaus Verbesserungspotential.

SIM Alert

Diese Funktion sendet ein Email an den Nutzer sobald ein Wechsel der SIM Karte durchgeführt wird. Dies hat in unserem Test sehr stabil funktioniert. Das Gerät wird hierbei nicht gesperrt.

Safe Browsing

Ganz unscheinbar (nur ein Schaltknopf in den Einstellungen) liefert CheetahMobile eine Safe Browsing Funktion mit. Vor welchen Gefahren CM Security genau schützt konnten wir nicht herausfinden. In unserem Kurztest mit URLs zu Phishingseiten hat diese auch einwandfrei funktioniert.



Call Blocking

Diese Komponente kann die Anrufe von bestimmten Nummern unterdrücken. Hierfür muss der Nutzer angeben, welche Nummern blockiert werden sollen (Blacklisting). Nummern können entweder manuell eingegeben oder aus den Kontakten und Anruflogs importiert werden.

In unseren Tests hat diese Komponente gut funktioniert. Achtung jedoch beim Format der Telefonnummer bei manueller Eingabe. Die Komponente blockt den Anruf nur, wenn das Format mit Ländervorwahl, jedoch ohne führenden Nullen angegeben wird (z.B. 43699123...).

Updates

Updates können manuell durch Anklicken des Update-Buttons durchgeführt werden. Zusätzlich werden automatische Updates angeboten. Informationen über das Intervall der Updates werden nicht gegeben.

Hilfe

Wir konnten keinerlei Hilfe finden.

Deinstallation

Die Deinstallation der Anwendung kann über die androidinterne Anwendungsverwaltung

deinstalliert werden. Hierfür ist keine Passworteingabe notwendig. Dies kann ein Problem sein, denn ein Dieb könnte so den Diebstahlschutz einfach deaktivieren.

Lizenz

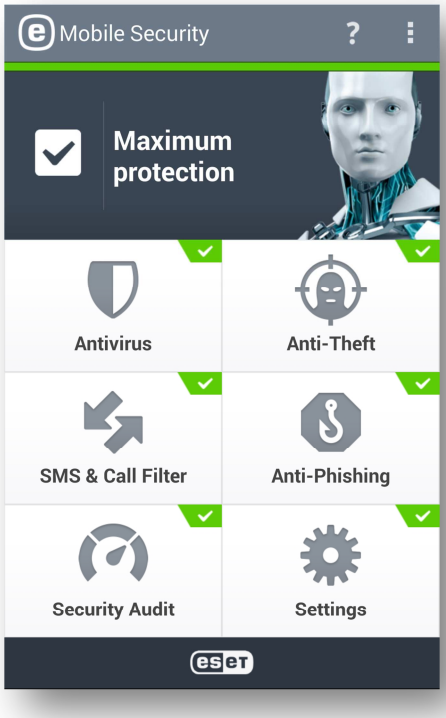
CheetahMobile bietet CM Security kostenlos an.

Fazit

CM Security ist ein durchaus ausgereiftes Sicherheitsprodukt. Der Diebstahlschutz hat insgesamt sehr gut und stabil funktioniert. Gefallen hat uns, dass im Grunde jede Funktion, die implementiert wurde, ausgereift ist und in hoher Qualität ausgeführt wurde. Dies kann man jedoch nicht über die Wipefunktion behaupten, welche durchaus noch überarbeitet werden sollte.

ESET Mobile Security

ESET bietet mit ESET Mobile Security ein Securityapp, welches über Antivirus und Anti-Theft Komponenten verfügt. Zusätzlich werden in der Premium Version noch SMS und Call Filter, Anti-Phishing, eine System Audit Komponente, erweiterte Diebstahlsicherung und ein SIM-Guard angeboten. Im Vergleich zur Vorjahresversion wurde das Programm mit einem Webinterface erweitert.



Installation

ESET Mobile Security wurde über den Google Play Store installiert. Beim ersten Start der App wird der Nutzer dazu aufgefordert den Lizenz-Vereinbarungen zuzustimmen. Des Weiteren ist es möglich einen Haken zu setzen, welcher standardmäßig deaktiviert ist, um ESET mit dem Senden von anonymen Daten betreffend der Nutzungsweise der Applikation zu unterstützen. Nach dieser ersten Konfiguration ist es möglich *ESET Live Grid* zu deaktivieren (Standard ist aktiv). Hierbei handelt es sich um eine Art Frühwarnsystem, welches aktuell gesammelte Daten von allen Teilnehmern des Systems verwendet. Im darauffolgenden Schritt kann der Nutzer entscheiden, ob ESET auf PUA (Potentially unwanted applications) reagieren soll. Abschließend wird die Lizenz überprüft und wir bekommen die Meldung, dass ESET nun einen ersten Scan starten wird.

Starten des Programms

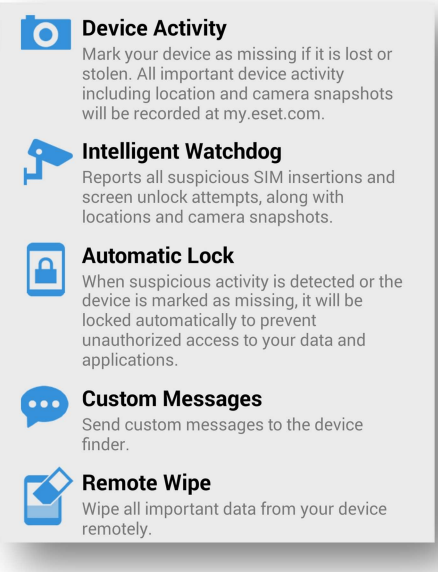
Nach der Erstkonfiguration wird der Nutzer auf einen übersichtlichen Startbildschirm weitergeleitet. Von hier aus hat er Zugriff auf die einzelnen Komponenten der Software. Aktive Komponenten sind mit einem grünen Haken gekennzeichnet, inaktive mit einem grauen Schaltknopf. Es ist möglich die Premium Version 30 Tage lang kostenlos zu testen. Hierfür wird eine Emailadresse benötigt. Im oberen Teil des Bildschirms werden ein Haken und eine Statusmeldung „Maximum protection“ eingeblendet. Dies könnte einen falschen Eindruck vermitteln, denn bis auf die Antiviruskomponente sind alle enthaltenen Funktionen inaktiv.

Antivirus

Die Antivirus Funktion bietet die Möglichkeit das System auf Malware zu scannen. Hierfür ist es möglich die Tiefe des Scans einzustellen. Zusätzlich zu manuellen Scans können automatische Scans definiert werden. Sinnvoll ist auch die Funktion „On-Charger Scan“, welcher automatisch beim Anstecken des Ladegerätes einen Scan startet. Außerdem ist es möglich die Quarantäneliste, die Liste der ignorierten Gefahren, Scan Logs und Updatedetails zu betrachten. Des Weiteren kann die Virendefinition durch einfaches Tippen aktualisiert werden. Die erweiterten Einstellungen ermöglichen das Aktivieren von automatischen Updates (zwischen sechs Stunden und zwei Wochen), sowie Einstellungen bezüglich Echtzeiterkennung und ESET Live-Grid. Außerdem kann die Standardaktionen bei Malwarefunden gesetzt werden. Hierfür werden die Aktionen „Entfernen“ und „Quarantäne“ angeboten.

Anti Theft

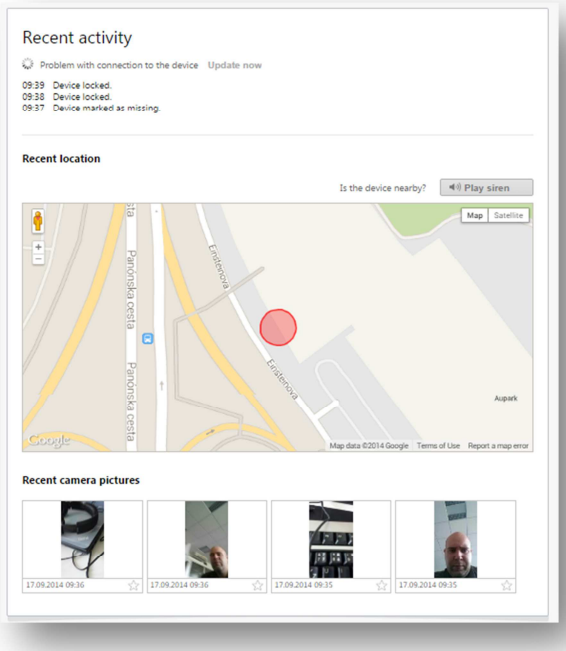
Beim ersten Start der Anti-Theft Komponente muss diese aktiviert werden. Hierfür bietet ESET einen komfortablen Assistenten an. Als erster Schritt ist es nötig ein Sicherheits-Passwort anzulegen (mindestens vier Zeichen). Zusätzlich kann eine Erinnerungsphrase angeben werden. ESET weist darauf hin, dass kurze Kennwörter unsicher sind. Um eine unautorisierte Deinstallation zu verhindern, fordert ESET den Nutzer dazu auf das Produkte als Geräteadministrator einzutragen. Im Anschluss wird die aktuelle SIM-Karte als vertrauenswürdige SIM eingetragen. Zudem muss die Nummer eines Freundes gespeichert werden. Gefallen hat uns, dass der Anzeigetext bei gesperrtem Gerät eingegeben werden kann. Um SMS Kommandos verwenden zu können wird ein Passwort benötigt. Es wird empfohlen dafür ein eigenes Passwort zu generieren, es besteht aber auch die Möglichkeit das Sicherheits-Passwort zu verwenden.


Device Activity
Mark your device as missing if it is lost or stolen. All important device activity including location and camera snapshots will be recorded at my.eset.com.
Intelligent Watchdog
Reports all suspicious SIM insertions and screen unlock attempts, along with locations and camera snapshots.
Automatic Lock
When suspicious activity is detected or the device is marked as missing, it will be locked automatically to prevent unauthorized access to your data and applications.
Custom Messages
Send custom messages to the device finder.
Remote Wipe
Wipe all important data from your device remotely.

ESET bietet seit diesem Jahr auch ein Webinterface für die Verwaltung und den Diebstahlschutz an. Hierfür kann während der Installation ein Nutzerkonto angelegt werden. Somit wurde die Aktivierung von Anti-Theft abgeschlossen.

Nach dem Abschluss des Vorgangs wird das Menü von Anti-Theft angezeigt. Der Eintrag „Optimization“ sticht hervor, da er orange hinterlegt wurde und mit einem Ausrufezeichen darauf hinweist, dass es ein Problem gibt. Nach Antippen des Icons meldet ESET, dass kein Lockscreen aktiviert wurde. Deshalb werden auch nur vier von fünf Sternen für die Sicherheit vergeben. Nach dem Setzen eines Sperrbildschirms wird die volle Punktezahl vergeben. Als weitere Indikatoren für die Sicherheit nennt ESET: Ortungsdienste aktiviert, GPS aktiviert, Screenlock aktiviert, Mobile Daten aktiviert, Google Play Services präsent.

Alle Befehle für Anti-Theft können per SMS oder per Webinterface (http://my.eset.com) abgesetzt werden. Im Webinterface muss das Gerät als „vermisst“ gemeldet werden um auf die Diebstahlschutzfunktionen zugreifen zu können. Dies leitet automatisch alle wichtigen Schritte ein, welche im Fall eines Diebstahls durchzuführen sind: Sperren, Lokalisieren und Fotos erstellen – jeweils in regelmäßigen Abständen. Schick gemacht.



SIM Guard

Diese Funktion soll vor unbefugtem Wechsel der SIM-Karte schützen. Wird eine SIM-Karte

eingelegt, die nicht hinterlegt ist, wird das Smartphone gesperrt. Diese Funktion hat in unseren Tests einwandfrei funktioniert und wir hatten immer noch die Möglichkeit durch Eingabe des Sicherheits-Passwortes die Sperre aufzuheben oder Notrufnummern zu wählen. Im Vergleich zur Vorjahresversion wurde nach fünf falschen Passworteingaben eine Wartezeit eingeführt. Dies soll Bruteforce-Attacken erschweren.

Lock

SMS Kommando: eset lock <password>

Dieses Kommando sperrt das Gerät und verhindert somit den Zugriff für Unbefugte. Beim Sperren des Geräts per SMS erhält der Absender eine Antwort mit der IMEI- des Geräts und IMSI-Nummer der SIM Karte. Der Lock ist sehr robust gestaltet, wir konnten ihn nicht umgehen. Außerdem ist es möglich sowohl Notrufe zu tätigen, als auch den Besitzer zu kontaktieren.

Sirene

SMS Kommando: eset siren <password>

Dieses Kommando lässt eine sehr schrille Sirene ertönen und sperrt das Gerät gleichzeitig. Dies kann zum Beispiel beim Wiederfinden eines verlegten Geräts helfen oder einen Dieb dazu motivieren das Diebesgut loszuwerden.

Find

SMS Kommando: eset find <password>

Durch Absenden des Befehls per SMS wird an den Absender ein Link von Google Maps mit Koordinaten gesendet. Im Webinterface wird kontinuierlich geortet. Somit sind immer mehrere Standorte verfügbar und der Bewegungsverlauf des Geräts kann verfolgt werden.

Wipe

SMS Kommando: eset wipe <password>

Diese Funktion löscht alle persönlichen Daten des Nutzers vom Mobiltelefon. Hierbei wird das Gerät nicht auf Werkseinstellungen zurückgesetzt, was den Vorteil hat, dass der Diebstahlschutz weiterhin aktiv bleibt. Dennoch wurden in unserem Test alle wichtigen Daten, jedoch nicht die SMS, gelöscht. Hier sollte noch ein wenig nachgebessert werden. Auf dem alternativen Gerät mit Android Version 4.1.2 wurden die SMS jedoch wie gewünscht entfernt.

Sonstige Funktionen

Sollte das Gerät als gestohlen gemeldet sein, erstellt ESET automatisch Fotos mit der Frontkamera des Geräts. Diese sind anschließend im Webinterface sichtbar. Somit lässt sich zum Beispiel ein Dieb identifizieren. Außerdem werden die Netzwerke erfasst, in welche sich das Gerät einbucht. Somit können Rückschlüsse gezogen werden, in welchem Umfeld sich das Gerät gerade aufhält.
Zusätzlich lassen sich alle erfassten Daten exportieren und als ZIP Datei herunterladen. Diese können dann etwa der Polizei übergeben werden um nach einem Dieb zu fahnden.

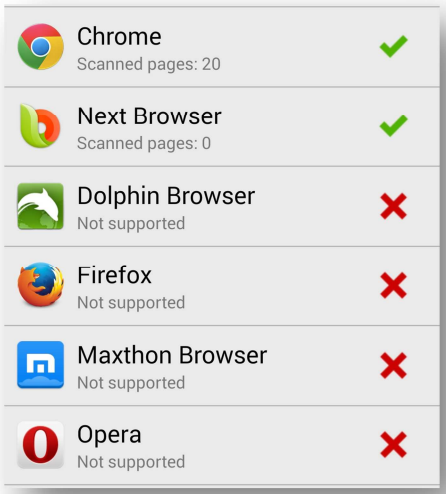
SMS & Call Filter

Diese Funktion bietet die Möglichkeit sehr umfangreiche Regeln zum Black- und Whitelisting von Anrufen und Nachrichten festzulegen. Es ist möglich eine Regel zu erstellen, die bestimmt was von welchen Nummern zu was für einem Zeitpunkt geblockt oder durchgelassen werden soll. Es kann sowohl eine Regel für konkrete Nummern erstellt werden, als auch für unbekannte Anrufer, wie zum Beispiel solche mit versteckter Nummer.
In unserem Test zeigte uns ESET eine Meldung, dass das Blockieren von SMS mit dem System unseres Gerätes nicht funktioniert. Anrufe hingegen wurden wie erwartet abgewiesen. Auf dem alternativen Testgerät mit Android Version 4.1.2 wurden auch SMS geblockt.

Anti Phishing

Anti-Phishing schützt den Benutzer beim Surfen im Internet. ESET überprüft alle installierten Browser auf Kompatibilität. ESET gibt an, dass diese Funktion mit den

gängigsten Browsern kompatibel ist. In der Praxis bedeutet dies, Google Chrome und der Next Browser unterstützt werden, andere wie Opera, Firefox, Dolphin und Maxthon jedoch nicht.



Der Phishingschutz hat in unserem Test mit Google Chrome einwandfrei funktioniert. Es erscheint eine Meldung, dass ESET empfiehlt die Seite unverzüglich zu verlassen. Beim Next Browser, welcher laut Information von ESET auch unterstützt werden sollte, konnten wir keine Detektion provozieren. Auch die Anzahl der analysierten Seiten bleibt auf „0“. ESET hat uns darüber informiert, dass es sich hier wohl um einen Anzeigefehler handelt. Next Browser wird nicht unterstützt, was in kommenden Versionen auch entsprechend signalisiert werden wird.

Security Audit

Das Security Audit gibt Information über Systemeinstellungen und Programmrechte welche ein Sicherheitsrisiko darstellen können. Wir wurden in unserem Test unter anderem darauf aufmerksam gemacht, dass der USB-Debug-Modus sowie die Installation aus unbekannten Quellen aktiviert sind. Die Komponente bietet auch Benachrichtigungen bezüglich unsicheren WiFi Netzen, aktiviertem Roaming bei Anrufen und Datenverkehr, sowie der Speichernutzung.

In einer Application Audit werden Apps in fünf Kategorien von möglichen Privatsphäreverletzungen eingeteilt. Die Kategorien sind Bezahldienste, Ortungsdienste, Abrufen der Identität, das Abrufen von Nachrichten sowie das Abrufen von Kontakten.

Updates

Updates werden automatisch durchgeführt. Der Nutzer kann das Intervall hierfür einstellen. Verfügbare Intervalle sind sechsstündig, täglich, jeden 3. Tag, wöchentlich und zweiwöchentlich. Zusätzlich kann manuell aktualisiert werden.

Hilfe

Für jede Ansicht im Userinterface lässt sich durch ein Tippen auf das Fragezeichensymbol eine detaillierte Hilfe aufrufen. Diese beschreibt jeweils die aktuelle Ansicht und bietet ausreichende Detailtreue.

Deinstallation

Für die Deinstallation wird ein Assistent angeboten, welcher alle nötigen Schritte einleitet. Zuvor muss das Kennwort für den Diebstahlschutz eingegeben werden. Somit kann ein Dieb das Produkt nicht einfach Deinstallieren.

Lizenz

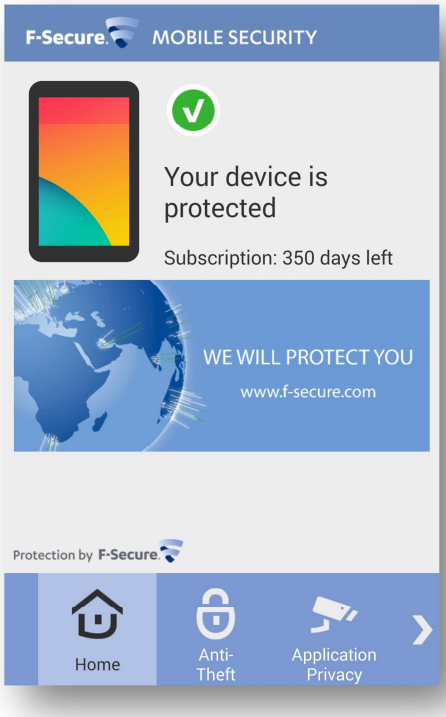
Eine Version mit eingeschränktem Funktionsumfang ist kostenlos verfügbar. Für Premiumfunktionen wie zeitgesteuerte Scans, Phishing Schutz, Automatische Malwaredatenbankupdate, Diebstahlschutz (Webinterface, SIM Guard, Wipe), SMS & Call Filter und Security Audit muss eine Premium Version erworben werden, welche für 9,99€ pro Jahr verfügbar ist.

Fazit

ESET Mobile Security war bereits im vorjährigen Test ein Produkt, welches einen großen Funktionsumfang gepaart mit Bedienbarkeit bietet. Das neu hinzugekommene Webinterface rundet das Produkt ab. Insgesamt konnte das Produkt im Test überzeugen. Alle Funktionen wurden solide ausgeführt.

F-Secure Mobile Security

F-Secure Mobile Security ist ein Sicherheitsprodukt welches alle wichtigen Funktionen bereitstellt. Zusätzlich bietet es sinnvolle Zusatzfunktionen wie Kindersicherung und Browserschutz runden das Sicherheitsprodukt ab.



Installation

F-Secure Mobile Security wurde aus dem Google Play Store bezogen und installiert. Im ersten Schritt müssen die Lizenzvereinbarungen akzeptiert werden. Daten werden anonymisiert an F-Secure übertragen, es sein denn der Nutzer entfernt den standardmäßig aktivierten Haken in der Checkbox.

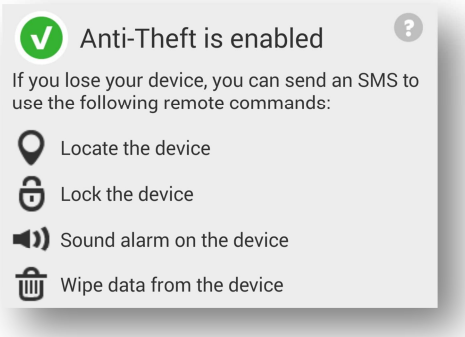
Anschließend wird die 30-tägige Testversion aktiviert. Im Zuge dessen wird die Applikation als Geräteadministrator eingetragen. F-Secure empfiehlt das Scannen des Geräts.

Starten des Programms

Nach dem ersten Start des Programms Erscheint eine Meldung, dass einige Dienste nicht aktiviert wurden. Dies wird uns im Menü-Slider durch ein Ausrufezeichen neben der Anti-Theft Komponente signalisiert.

Anti-Theft

Die Diebstahlschutzkomponente ist standardmäßig deaktiviert. Sie wird nur mit SMS Kommandos gesteuert. Ein Webinterface ist nicht verfügbar. Vor der Einrichtung muss die Android-interne Bildschirmsperre aktiviert werden. Dieser Schritt kann übersprungen werden, F-Secure weist jedoch darauf hin, dass dann ein Dieb die Diebstahlsicherung leicht deaktivieren kann. Anschließend muss ein Sicherheitscode festgelegt werden. Dieser muss aus mindestens fünf Zeichen bestehen. Außerdem darf er nicht zu simpel sein. „qqqqq“ wurde nicht akzeptiert. Anschließend muss die Emailadresse angegeben werden, welche als Empfänger für Instruktionen dient, sowie eine vertrauenswürdige Telefonnummer, welche bei einem SIM-Kartenwechsel informiert wird. Die verfügbaren SMS Kommandos sind in der Hilfe einsehbar. Für das Ändern der Einstellungen muss das Kennwort eingegeben werden.


Anti-Theft is enabled
If you lose your device, you can send an SMS to use the following remote commands:
Locate the device
Lock the device
Sound alarm on the device
Wipe data from the device

Lock

SMS Kommando: „#lock#<Passwort>“

Mit diesem Kommando wird der Bildschirm mit Hilfe des in Android integrierten Sperrbildschirms gesperrt. Dieser ist sehr robust, somit ist es Dritten unmöglich auf das Gerät zuzugreifen. Als Antwort erhält der Sender der SMS einen Link auf Google Maps mit den aktuellen Koordinaten des Geräts.

Locate

SMS Kommando: „#locate#<Passwort>“

Diese Funktion dient dem Wiederfinden eines verlorenen oder gestohlenen Smartphones.

Nach dem Senden dieses Befehles erhält der Sender ein SMS mit den Koordinaten des Telefons und einem Link auf Google Maps. Zusätzlich wird das Gerät gesperrt. Es besteht also kein Unterschied zwischen Lock und Locate.

Alarm

SMS Kommando:

„#alarm#<Passwort>#<Count>“

Dieser Befehl funktioniert auf dieselbe Art und Weise wie der Lock Befehl, jedoch wird zusätzlich ein Alarm ausgelöst. Mit dem Paramater *Count* kann die Anzahl der Alarme bestimmt werden. Ohne Angabe des Parameters dauert der Alarm unendlich an, mit der Angabe von „0“ schaltet man den Alarm aus.

Wipe

SMS Kommando: „#wipe#<Passwort>“

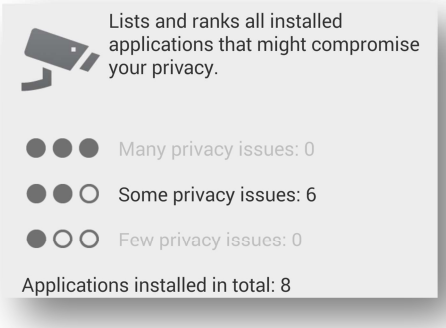
Dieser Befehl dient dem Löschen aller persönlichen Daten die sich auf dem Handy befinden. Hierfür wird zuerst die externe SD-Karte gelöscht und im Anschluss das Gerät auf Werkseinstellungen zurückgesetzt. In unserem Test wurden alle Daten gelöscht. Ein Wiederherstellen von Daten auf der externen SD-Karte war mit einem kostenlosen Tool nicht möglich. Der gesamte Prozess war in wenigen Augenblicken abgeschlossen.

SIM Change

Diese Funktion sendet bei einem Wechsel der SIM Karte eine SMS an die eingetragene vertrauenswürdige Nummer. Dies kann zum Beispiel sinnvoll sein, wenn ein Dieb versucht seine eigene SIM Karte in das Gerät einsteckt.
In unserem Test hat diese Funktion nicht richtig funktioniert. Obwohl wir das Szenario mehrmals nachgespielt haben konnten wir keine SMS empfangen. Auf unserem alternativen Gerät mit Android 4.1.2 hat die Funktion jedoch einwandfrei funktioniert.
Nachdem wir F-Secure über den Missstand informiert haben, hat der Hersteller schnell reagiert und eine neue Version veröffentlicht, welche das Problem behebt.

Application Privacy

Diese Funktion scannt alle installierten Applikationen auf mögliche Verletzungen der Privatsphäre. Hierbei teilt F-Secure die Risiken in „viele“, „einige“ und „wenige“ Probleme ein. Durch Antippen einer Kategorie werden jeweils die Applikationen angezeigt. Gut gefallen hat uns, dass F-Secure die Berechtigungen der Applikationen vereinfacht darstellt. So ist zum Beispiel die Berechtigung „ACCESS_FINE_LOCATION“ in der Liste als „Knows where you are“ eingetragen.


Lists and ranks all installed applications that might compromise your privacy.
Many privacy issues: 0
Some privacy issues: 6
Few privacy issues: 0
Applications installed in total: 8

Zusätzlich wird eine ausführliche Beschreibung zu der Berechtigung gegeben. Sollte der Nutzer vermuten, dass eine Verletzung der Privatsphäre vorliegt kann er direkt eine Deinstallation vornehmen.

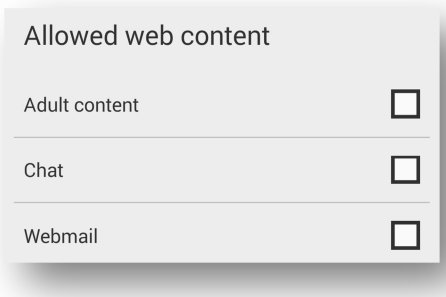
Anti-Virus

Diese Komponente schützt das System vor Malware. Das Datum des letzten Scans, sowie des letzten Updates werden angezeigt. Es besteht einerseits die Möglichkeit manuell das ganze Gerät zu scannen oder automatische Scans zu planen. Für die Frequenz dieser Überprüfungen ist täglich, wöchentlich und monatlich wählbar. Auch der Wochentag und der Zeitpunkt kann eingestellt werden.
Außerdem ist es möglich Cloud Protection zu deaktivieren oder nur zu verwenden wenn keine Roaming Gebühren anfallen würden. Zusätzlich haben besteht die Möglichkeit dem Real-Time Protection Network beizutreten (Standardmäßig aktiv). Dieses analysiert Dateien und soll gegen die aktuellsten Gefahren schützen. F-Secure gibt an, dass

hierbei anonymisierte Daten übertragen werden um den Dienst laufend zu verbessern.

Parental Control

Diese Komponente dient dazu unangemessene Inhalte des Internets für Kinder unzugänglich zu machen. Gleiches gilt für installierte Applikationen. Der Nutzer hat die Möglichkeit zwischen den Profilen *Child*, *Teen* und *Adult* zu wählen, die jeweils einen anderen vorkonfigurierten Grad an Filterung anbieten. Dieser kann individuell angepasst werden. So ist es z.B. möglich Inhalte wie z.B. Waffen, Glücksspiel oder Illegale Downloads zu sperren. Für jegliche Änderungen für die Kindersicherung ist ein Kennwort erforderlich, sodass der Sprössling nicht einfach den Schutz deaktivieren kann.



Auch wählbar sind die für Kinder erlaubten Applikationen. Standardmäßig sind alle aktiviert. Eltern können bestimmte Apps abwählen, für welche beim Öffnen ein Kennwort erforderlich sein soll.

Safe Browsing

F-Secure schützt den Nutzer während des Browsens im Internet vor Gefahren wie Phishing und Schadsoftware. Es wird ein eigener Safebrowser mitgeliefert. Im letztjährigen Test haben wir bemängelt, dass der Nutzer nur während dem Browsen im F-Secure Safe Browser geschützt war. F-Secure hat hier nachgebessert und schützt den Nutzer nun zusätzlich bei der Verwendung von Google Chrome und Dolphin. In unserem Test hat der Schutz funktioniert.

Safe Contacts

Mit dieser Funktion ist es möglich Anrufe und SMS von bestimmten Teilnehmern zu blockieren. Für die Konfiguration können Nummern entweder manuell eingetragen oder aus den Kontakten oder dem Gesprächsverlauf importiert werden. Das Blockieren geschieht mittels einer einfachen Blacklist. Fügt man eine Nummer zu dieser Liste hinzu werden alle ein- und ausgehenden Anrufe, sowie eingehende SMS dieser Nummer geblockt. Es ist nicht möglich nur SMS oder nur Anrufe zu blocken.

In unserem Test hat das Blockieren von Telefonanrufen gut funktioniert, das Blockieren von SMS jedoch nicht. Auf unserem alternativen Gerät mit Android hat die Funktion jedoch einwandfrei funktioniert.

Updates

Updates werden automatisch durchgeführt. Hierbei kann der Nutzer einstellen, ob diese nur beim eigenen Provider, oder bei allen durchgeführt werden sollen.

Hilfe

Zu jeder Funktion kann mithilfe des Fragezeichensymbols ein Hilfefenster an. In diesem findet der Nutzer detaillierte Anleitungen, die ausreichende Informationen bieten sollten.

Deinstallation

Die Deinstallation ist passwortgeschützt. Unter dem Menüpunkt More > Uninstall findet der Nutzer einen Deinstallationsassistenten. Nach Eingabe des Passwortes wird das Programm direkt entfernt. Um das Programm über den Android App Manager zu deinstallieren, muss es erst aus den Geräteadministratoren ausgetragen werden, wofür ebenfalls ein Passwort erforderlich ist.

Lizenz

F-Secure ermöglicht dem Nutzer alle Funktionen für 30 Tage zu testen. Nach Ablauf dieser Zeit muss für die weitere Verwendung

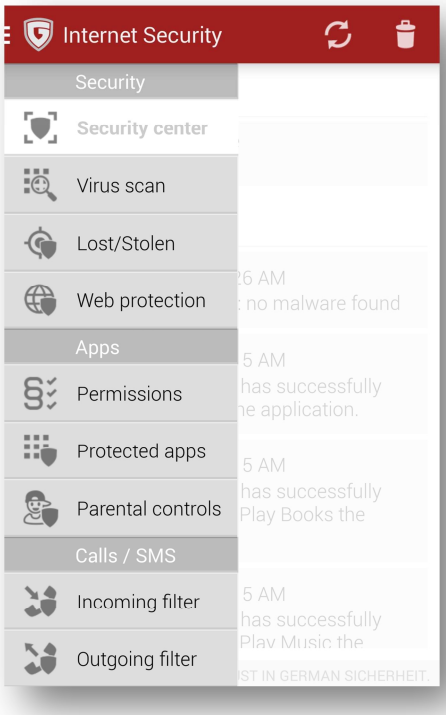
eine Lizenz für 7,45€ erworben werden, die für sechs Monate gültig ist.

Fazit

F-Secure hat im Test ein gutes Bild gemacht. Simple Navigation, sowie die Kindersicherung haben einen guten Eindruck hinterlassen. Safe Browsing wurde sinnvollerweise auf alternative Browser erweitert.

G Data Internet Security

G Data Internet Security bietet Virenscanner und einen Diebstahlschutz welcher per SMS gesteuert wird. Zusätzlich hat sich G Data auf den Schutz von Kindern spezialisiert. So ist ein Kid's Browser, ein Children's corner und weitere Funktionen, welche hilfreich für den Schutz von Kindern sein können, inkludiert.



Installation

G Data Internet Security wurde aus dem Google Play Store bezogen und installiert. Als erster Schritt muss der Name, sowie die Emailadresse eingegeben werden. Dort kann auch ein Lizenzschlüssel eingegeben oder die 30-tägige Testversion aktiviert werden. Außerdem muss der Nutzer die Lizenzvereinbarungen akzeptieren und kann entscheiden ob die angegebenen Daten für Werbung verwendet werden dürfen (Opt-out). Anschließend wird der Diebstahlschutz konfiguriert. Hierfür muss ein mindestens vierstelliger PIN festgelegt werden. Außerdem wird die Telefonnummer einer Vertrauensperson abgefragt, welche etwa ein vergessenes Passwort zurücksetzen kann oder im Falle eines SIM-Kartenwechsels benachrichtigt wird. Anschließend wird G Data Internet Security als Geräteadministrator eingetragen. Somit ist das Setup abgeschlossen.

Starten des Programms

Beim ersten Start des Programms führt G Data ein Update durch. Außerdem macht das Sicherheitsprodukt darauf aufmerksam, dass ein initialer Scan durchgeführt werden soll. Hierfür kann der Nutzer entscheiden, ob nur installierte Applikationen, oder ein Systemscan durchgeführt werden soll.
Anschließend wird auf dem Startbildschirm, dem Security Center, wird angezeigt, dass alles in Ordnung ist.

Virus Scan

Die Virusscan-Komponente ermöglicht es dem Nutzer sein Smartphone auf Schadsoftware zu überprüfen. Hierbei kann er entweder nur die installierten Applikationen oder das gesamte System scannen. Die Resultate werden im Security Center angezeigt.
In den Einstellungen kann ein automatischer, zeitgesteuerter Scan aktiviert werden. Für die Frequenz kann 1,3,7,14 oder 30 Tage gewählt werden. Gefallen hat uns, dass eingestellt werden kann, dass ein Scan nur bei ausreichend hohem Batteriestand durchgeführt wird. Außerdem kann festgelegt werden, dass der Scan nur während dem Aufladen des Smartphones stattfinden soll.

Lost/Stolen

Dieser Teil der Anwendung kann dem Nutzer helfen sein verlorengegangenes oder gestohlenes Smartphone wiederzuerlangen. Hierfür kommen SMS Befehle zum Einsatz, ein Webinterface ist nicht vorhanden. In den Einstellungen kann der Nutzer festlegen, welche Aktionen per SMS durchgeführt werden dürfen. Alle sind standardmäßig deaktiviert.

Locate telephone

SMS Kommando: <PIN> locate

Die Locate Funktion ortet das Gerät und sendet eine Antwort-SMS an den Sender des

Befehls mit den Koordinaten, sowie der MAC Adresse des Routers, mit dem das Gerät verbunden ist. Sinnvoller wäre unserer Meinung nach der Versand eines Direktlinks auf einen Kartendienst, denn die Handhabung von Koordinaten dürfte nicht für alle Nutzer geläufig sein. Zusätzlich zur SMS Antwort wird ein Email an den Nutzer gesendet. In diesem ist ein Link zu Google Maps enthalten. In den Einstellungen lässt sich zusätzlich die Option setzen, dass das Handy automatisch geortet wird, wenn die Batterie des Geräts schwach ist.

G Data hat sich diesbezüglich geäußert, dass dieser Weg gewählt wurde, da Links zu Google Maps in der Regel länger als 160 Zeichen lang sind und somit die maximale Länge von einzelnen SMS überschreiten würde. Auf externe URL Kürzungsdienste wolle man sich nicht verlassen.

Delete personal data

SMS Kommando: <PIN> wipe

Dieses Kommando löscht die persönlichen Daten des Nutzers vom Smartphone. Hierfür wird das Gerät auf Werkseinstellungen zurückgesetzt. Die Funktion hat wie erwartet funktioniert, jedoch wurden auf unserem Testgerät keine Daten auf der externen SD-Karte gelöscht.

Play ringtone

SMS Kommando: <PIN> ring

Dieses Kommando lässt einen Alarm auf dem Smartphone ertönen. Dieser stoppt erst, wenn die G Data Internet Security Applikation gestartet wird.

Set phone to mute

SMS Kommando: <PIN> mute

Dieses Kommando setzt das Gerät auf lautlos. Dies klappte in unseren Tests auch einwandfrei.

Lock screen

SMS Kommando: <PIN> lock

Dieses Kommando sperrt das Gerät des Nutzers mit dem Android Sperrbildschirm. Als PIN wird jener verwendet, welcher für die Diebstahlschutzkomponente definiert wurde.

Set device password

SMS Kommando: <old PIN> set device password: <new PIN>

Dieser Befehl ermöglicht das Setzen eines neuen PINs. Hierfür muss der alte bekannt sein.

Remote password reset

SMS Kommando: remote password reset: <new PIN>

Dieses Kommando ermöglicht das Zurücksetzen des Passworts, etwa wenn es vergessen wurde. Dieser Befehl wird nur von der Nummer der Vertrauensperson akzeptiert.

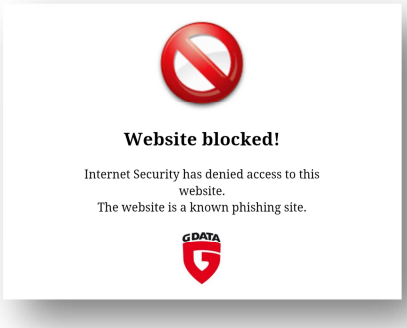
SIM Lock

Diese Komponente sperrt das Gerät wenn eine fremde SIM Karte eingelegt wird, etwa wenn ein Dieb seine eigene verwendet. Zusätzlich wird die Vertrauensperson per SMS verständigt. Optional kann das Gerät in einem derartigen Fall auch geortet werden.

Web protection

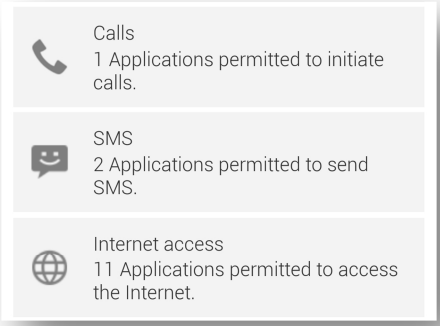
Die Web Protection Komponente schützt den Nutzer während dem Surfen im Internet mit dem Android und Chrome Browser. G Data gibt an, dass gegen Phishingattacken geschützt wird, was im Incognitomodus jedoch nicht verfügbar ist. In den Einstellungen kann festgelegt werden, dass die Web protection nur bei aktiver WLAN Verbindung tätig sein soll.

In unserem Kurztest hat diese Komponente gut funktioniert.



Permissions

Die Permissions Komponente zeigt installierte Applikationen auf, welche besondere Berechtigungen besitzen. Alle installierten Apps werden in Kategorien eingeteilt, wie zum Beispiel „Zugriff auf das Internet“ oder „Berechtigung zur Ortung“.



Durch Antippen einer dieser Einträge werden die entsprechenden Applikationen aufgelistet. Durch Antippen einer App, werden Details zu den Berechtigungen angezeigt, was unserer Ansicht nach sehr übersichtlich gestaltet wurde. Die Applikation kann aus dieser Ansicht direkt deinstalliert, oder zur „App protection“ hinzugefügt werden.

Protected apps

Die App protection schützt Applikationen vor unbefugtem Zugriff. Ein Anwendungsfall hierfür wäre zum Beispiel, wenn der Nutzer auf dem Smartphone seines Kindes bestimmte Applikationen sperren möchte. So kann ein Passwort festgelegt werden, welches für die Ausführung ausgewählter Apps eingegeben werden muss. Sollte der Nutzer seinen PIN vergessen haben, so kann er sich diesen per Email zusenden lassen. Somit ist es wichtig, dass der Nutzer auch seine Emailapplikation mit einem Passwort schützt, sofern eine Emailadresse eingegeben wurde, welche mit dem Gerät synchronisiert wird. Auf diesen Zustand macht G Data nicht aufmerksam. Außerdem sollte das Sicherheitsprodukt selbst geschützt werden, um die Komponente nicht einfach löschen zu können. Dies empfiehlt auch G Data, ebenso wie die Android Einstellungen und den Google Play Store.

Parental Controls

Diese Komponenten wurde eingeführt um es Eltern zu ermöglichen das Smartphone für ihre Kinder sicherer zu machen.

Beim Setup empfiehlt das Security Produkt statt des originalen Launchers jenen von G Data zu verwenden. Dieser legt sich vor die Oberfläche von Android und blendet alle installierten Applikationen aus. Es ist lediglich möglich jene Apps auszuführen, welche von den Eltern als sicher eingestuft werden. Um den Modus wieder zu verlassen ist ein Kennwort erforderlich.

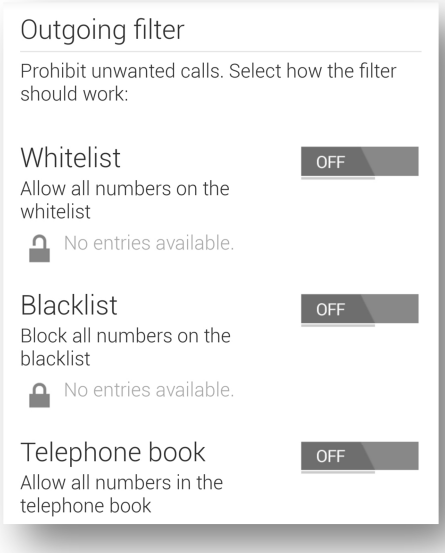
In unserem Test hat dies gut funktioniert. Einziger Schönheitsfehler war, dass es möglich war kurz zu den zuletzt geöffneten Applikationen zu wechseln. Nach weniger als einer Sekunde wurde aber wieder der Kid’s Corner angezeigt. Das Öffnen nicht erlaubter Applikationen war uns nicht möglich insofern handelt es sich hierbei nicht um einen schwerwiegenden Fehler.

Kid’s Browser

Der Kids Browser ist ein separates App, welches es speziell Kindern ermöglicht sicher Inhalte im Internet zu konsumieren. Es ist nur möglich ausgewählte Webseiten (genaue Liste unbekannt) zu öffnen. Diese sind durchwegs nur kinderfreundlich. Als Startseite ist http://fragfinn.de eingestellt, eine Suchmaschine, welche stets nur kinderfreundliche Ergebnisse liefert.

SMS & Call Filter

Dieser Teil der Applikation ermöglicht das Blockieren von unerwünschten Anrufen und SMS. Es ist möglich Regeln für die Blockierung eingehender Anrufe und SMS zu erstellen, sowie für ausgehende Anrufe.



Es kann entweder Black- oder Whitelisting eingestellt werden. Beim Blacklisting kann der Nutzer angeben, welche Nummern blockiert werden sollen. Alle anderen werden durchgelassen. Zusätzlich kann eingestellt werden, ob die Kontakte aus der Kontaktliste immer zugelassen werden sollen. Mit einer Checkbox kann der Nutzer entscheiden, ob unbekannte Nummern zugelassen werden sollen, oder nicht.

In unseren Tests hat diese Funktion verlässlich funktioniert. Nur das Blockieren von SMS hat nicht geklappt. Dies liegt wohl an der verwendeten Android Version (4.4). Auf unserem alternativen Testgerät mit Android Version 4.1.2 hat das Blockieren wie erwartet geklappt. G Data macht jedoch nicht darauf aufmerksam, dass diese Funktion mit der Android Version nicht kompatibel ist.

Einträge für die Black- und Whitelist können aus den Anruflogs und dem Adressbuch importiert oder manuell eingegeben werden.

Hide Contacts

Die Hide-Contacts-Komponente von G Data kann die Kommunikation mit bestimmten Kontakten, sowie die Kontakte selbst verstecken. Hierfür wird ein eigener Messenger geboten, welcher das Senden und Empfangen von SMS Nachrichten übernimmt.

In unserem Test hat diese Komponente nicht funktioniert. Sowohl ausgehende, als auch eingehende Nachrichten wurden angezeigt. Wir führen auch dies in auf eine inkompatible Android Version zurück. Auf unserem Testgerät mit Android 4.1.2 hat das Blockieren einwandfrei geklappt. G Data macht auch auf diesen Missstand nicht aufmerksam. Das Verstecken der Anruflogs hat hingegen einwandfrei funktioniert.

Updates

Updates werden automatisch durchgeführt. Als Intervalle können 1, 3, 7, 14 und 30 Tage gewählt werden. Außerdem kann eingestellt werden, dass Aktualisierungen ausschließlich über WLAN durchgeführt werden sollen.

Hilfe

Zu jeder Komponente wird meist eine kurze Erklärung im Menü geboten. Diese ist meist ausreichend. Eine explizite Hilfe in Form von Fließtext oder FAQ konnten wir jedoch nicht finden.

Deinstallation

G Data Internet Security kann über den Android Appmanager deinstalliert werden. Hierfür ist kein Passwort notwendig. Dies kann problematisch sein, wenn ein Dieb einfach den Diebstahlschutz deinstallieren kann.

Der Nutzer kann dem entgegenwirken, indem er die inkludierte App-Protection für die Android Einstellungen und das Security Produkt selbst aktiviert. G Data empfiehlt dies auch in den Einstellungen für App-Protection, standardmäßig ist dieses Verhalten jedoch nicht aktiv.

Lizenz

G Data Internet Security ist für 18,99€ pro Jahr im Google Play Store verfügbar. Eine Light-Version mit eingeschränktem

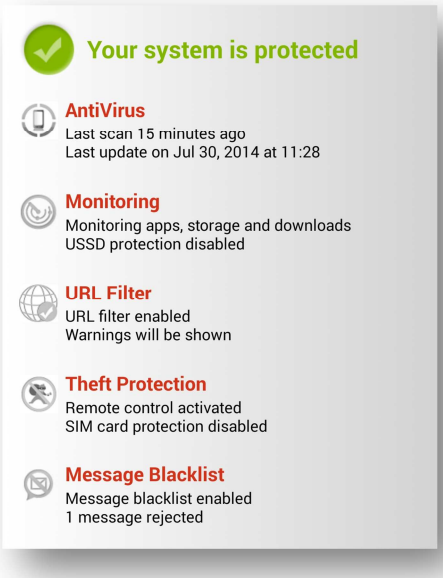
Funktionsumfang ist kostenlos verfügbar. Diese bietet Schutz vor gefährlichen Applikationen, sowie Berechtigungskontrolle. Die Testversion kann auf die Vollversion upgegraded werden.

Fazit

G Data Internet Security punktet vor allem mit der Kindersicherung, welche ausgereift wirkt. Zusätzlich ist ein solider Diebstahlschutz integriert. Die Wipefunktion sollte jedoch auch Daten auf der externen SD Karte berücksichtigen. Insgesamt wirkt das Programm jedoch solide.

Ikarus mobile.security

Ikarus bietet mit mobile.security ein übersichtliches Sicherheitsapp für Android Smartphones. Es verfügt über wichtige Sicherheitsfunktionen wie Virenscanner, Diebstahlschutz und URL Filter.



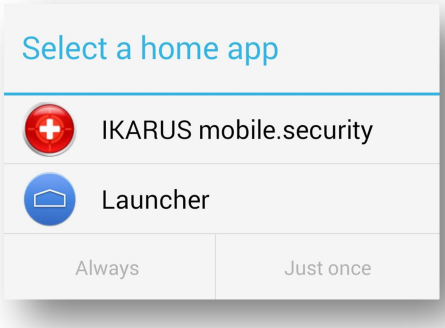
Installation

Ikarus mobile.security wurde aus dem Google Play Store heruntergeladen und installiert. Der Installationsvorgang ist verhältnismäßig lange, da dort alle nötigen Einstellungen vorgenommen werden.

Als erster Schritt müssen zunächst die Lizenzvereinbarungen akzeptiert werden. Danach führt IKARUS ein Update durch. Anschließend geht es an die Lizensierung. Der Nutzer hat die Möglichkeit das Produkt mittels Key (ist per QR Code scanbar), einem In-App Kauf über Google Play zu aktivieren, oder die 30 tägige Testversion zu nutzen. Alternativ kann er sich direkt für die kostenlose Variante entscheiden, die einen eingeschränkten Funktionsumfang bietet.

Im ersten Schritt wird die Anti-Theft Komponente konfiguriert. Der Nutzer kann sie entweder ein- oder ausschalten. Im ersten Fall wird das Securityprodukt als Geräteadministrator eingetragen.

Zusätzlich muss Ikarus als „Home App“ eingetragen werden.



Anschließend muss der Nutzer ein Passwort definieren, welches aus mindestens sechs Zeichen, einem Buchstaben und einer Ziffer bestehen muss. Nach erfolgreicher Konfiguration erhält der Nutzer noch eine kurze Einführung in die verfügbaren SMS Kommandos der Anti-Theft Komponente. Auch die Blacklisting Funktion, sowie der URL Filter, der beim Surfen im Internet schützt, wird direkt während der Installation aktiviert.

Nach Beendigung des Setups empfiehlt IKARUS einen initialen Malwarescan durchzuführen.

Starten des Programms

Beim Starten des Programms wird der Startbildschirm angezeigt. Am oberen Bildschirmrand kann der Nutzer den aktuellen Schutzstatus sehen, welcher in unserem Fall „Your System is protected“ lautet. Außerdem ist in dieser Ansicht direkt ersichtlich wann der letzte Malwarescan durchgeführt wurde, ebenso wie das Datum des letzten Updates.

AntiVirus

Die AntiVirus Komponente von IKARUS ermöglicht dem Nutzer das Scannen von allen installierten Apps, sowie des kompletten Systems. Außerdem kann ein automatischer Scan samt Frequenz eingestellt werden. IKARUS bietet hierfür zweimal täglich, täglich, jeden zweiten Tag oder wöchentlich als Optionen. Sollte das Gerät bereits einmal infiziert worden sein, können erkannte Infektionen eingesehen werden.

Am unteren Bildschirmrand befindet sich eine Checkbox die es dem Programm erlaubt

anonyme Statistiken zur Virenerkennung zum IKARUS Lab zu senden (Opt-Out).

Monitoring

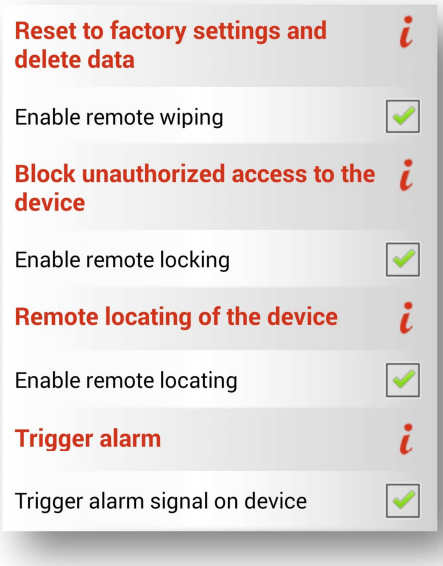
Unter Monitoring versteht IKARUS den Echtzeitschutz, welcher neue Apps, Veränderungen im Dateisystem sowie einen USSD Code Schutz betrifft. Jede dieser Unterfunktionen lassen sich separat ein- und ausschalten. Die ersten beiden sind standardmäßig aktiv, der USSD Blocker nicht.

URL Filter

Der URL Filter schützt den Nutzer beim Surfen im Internet vor gefährlichen Seiten. IKARUS geht dabei nicht darauf ein, welche Browser unterstützt werden. Es wird angegeben, dass Phishingseiten, sowie solche die Malware verbreiten, geblockt werden.

Theft Protection

IKARUS listet alle vorhandenen Diebstahlschutzfunktionen auf und ermöglicht die Deaktivierung jeder Komponente. Die Steuerung aller Diebstahlschutzfunktionen erfolgt über SMS, ein Webinterface wird nicht angeboten.


Reset to factory settings and delete data
Enable remote wiping
Block unauthorized access to the device
Enable remote locking
Remote locating of the device
Enable remote locating
Trigger alarm
Trigger alarm signal on device

Für die Deaktivierung einer Komponente ist jeweils das Passwort einzugeben, was grundsätzlich zu begrüßen ist, jedoch wäre es wohl praktischer den kompletten Dialog mit einem Passwort zu schützen anstatt den Nutzer bei jeder Checkbox das Kennwort erneut eingeben zu lassen. Dieses lässt sich übrigens in diesem Dialog ändern.

Wipe

SMS Kommando: „wipe: <Password>“

Dieses Kommando löscht alle persönlichen Daten vom Gerät, um sie bei Verlust oder Diebstahl für Dritte unzugänglich zu machen. Hierbei wird das Gerät auf Werkseinstellungen zurückgesetzt. Ikarus hat auch die Dateien von der externen SD Karte gelöscht. Diese konnten jedoch mit gängiger Freeware wiederhergestellt werden.

Lock

SMS Kommando: „lock: <Password>“

Sofort nach dem Absetzen des Kommandos wird das Gerät mit einem Lockscreen gesperrt. Der Absender bekommt dies durch eine SMS bestätigt. Der Lock war allgemein sehr sicher. Wir konnten ihn nicht umgehen. Außerdem konnte zu jedem Zeitpunkt ein Notruf abgesetzt werden.

Locate

SMS Kommando: „locate:<Password>“

Nach erfolgreicher Lokalisierung erhält der Sender eine Antwort mit einem Link auf Google Maps samt Koordinaten.

Alarm

SMS Kommando: „alarm: <Password>“

Dieses Kommando verhält sich genau gleich wie das Sperren, jedoch wird zusätzlich ein lautes Sirenengeräusch abgespielt. Dies funktioniert auch, wenn das Gerät auf Vibration gestellt ist.

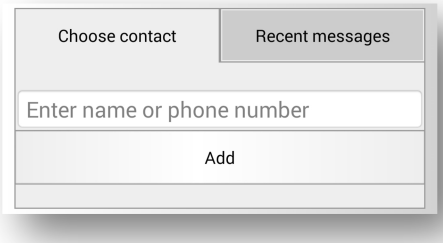
SIM Card Protection

Wird das Handy gestohlen und eine fremde SIM Karte eingelegt, wird es gesperrt und so der Zugriff auf Daten durch Dritte verhindert. Durch Eingabe des richtigen Kennwortes kann es dennoch verwendet werden.

Message Blacklist

Message Blacklisting verhindert das Empfangen von SMS von unerwünschten

Absendern. Das Userinterface ist sehr einfach gehalten und ermöglicht lediglich das Hinzufügen und Entfernen von Nummern.



Die Nummern können entweder direkt eingegeben oder aus den Kontakten importiert werden. Des Weiteren ist es möglich unter dem Reiter „*Recent Messages*“ Nummern von zuvor eingegangenen SMS einzusehen und direkt zu importieren. Gefallen hat uns die automatische Antwort, die bei einem Block an den blockierten Teilnehmer zurückgesendet wird. Diese kann durch den Nutzer frei definiert werden.
In unserem Test hat das Blockieren der SMS Nachrichten nicht funktioniert. Dies führen wir auf Inkompatibilität mit Android 4.4 zurück. Auf unserem alternativen Testgerät mit Android 4.1.2 hat die Funktion hingegen einwandfrei geklappt.

Info

Der Infobereich zeigt Versionsinformationen zum Produkt. Außerdem finden sich dort Kontaktmöglichkeiten in Form von Emailadressen und Telefonnummern. Außerdem kann der Systemlog z.B. als Email an den Support versandt werden.

Restart Setup

Für diese Aktion ist abermals das Passwort erforderlich. Anschließend wird die Konfiguration des Sicherheitsproduktes zurückgesetzt und der Nutzer durch dieselbe Konfigurationsanleitung geleitet wie bei der Erstinstallation.

Updates

Wie auch für die geplanten Scans können Updates automatisch durchgeführt werden. Hierfür sind dieselben Einstellmöglichkeiten verfügbar. Zusätzlich kann definiert werden, ob Updates nur bei WiFi Verbindung durchgeführt werden sollen, oder bei jeder Art der Internetverbindung. Zusätzlich können Updates manuell durchgeführt werden.

Hilfe

IKARUS unterstützt den Nutzer bei der Konfiguration durch kurze, aber informationshaltige Infoboxen. Auf der Homepage des Herstellers finden wir zwar diverse Handbücher zu anderen Produkten, jedoch keine zur Mobile Suite. Außerdem existiert ein FAQ mit einem Inhalt von ca. 20 Fragen, die jedoch eher oberflächlich sind.

Deinstallation

IKARUS mobile.security bietet einen Deinstallationsassistenten, der den Nutzer beim Deinstallieren unterstützt. Dazu muss das Passwort eingegeben werden. Anschließend wird das Programm nach einem kurzen Dialog ohne weiteres Zutun deinstalliert.

Es ist möglich das Sicherheitsprodukt auch ohne Passworteingabe mittels Android App Manager zu deinstallieren. Hier sehen wir ein grobes Sicherheitsproblem, da auf diese Art und Weise ein Dieb ohne weiteres den Diebstahlschutz komplett deaktivieren kann.

Lizenz

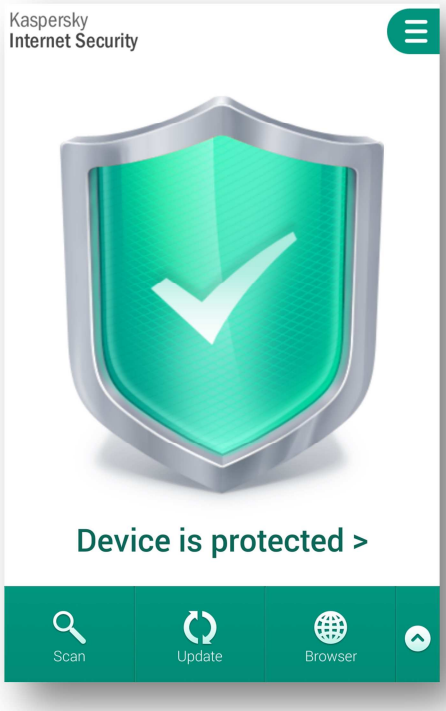
Ikarus bietet den Nutzern an, mobile.security für 30 Tage kostenlos zu testen. Nach diesem Zeitraum können Interessierte eine Lizenz für 19,95€ ohne zeitlicher Limitierung im Play Store oder auf der Herstellerwebseite für 9€ für ein Jahr erwerben.

Fazit

Ikarus mobile.security enthält alle wichtigen Sicherheitsfunktionen. Die Benutzeroberfläche wirkt aufgeräumt und sollte von jedem bedient werden können. Die implementierten Komponenten haben allgemein vernünftig funktioniert.

Kaspersky Internet Security

Kaspersky Internet Security wurde im Vergleich zur Vorjahresversion optisch überarbeitet. Dem Nutzer wird ein breites Spektrum an Funktionen geboten. Neben einem Virenscanner werden SMS & Call Filter, Browserschutz, Diebstahlschutz und mehr geboten.



Installation

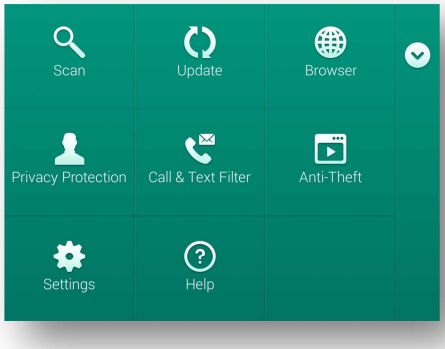
Kaspersky Internet Security wurde aus dem Google Play Store bezogen und installiert. Im ersten Schritt muss der Nutzer das Land, in dem er lebt, einstellen. Anschließend müssen die Lizenzvereinbarungen akzeptiert werden.

Starten des Programms

Nach dem Abschluss der Installation wird der Nutzer auf den Startbildschirm weitergeleitet. Hier wird sehr auffällig darauf aufmerksam gemacht, dass der Nutzer einen Sicherheitsscan des Geräts durchführen solle. Anschließend wird auf dem Startbildschirm signalisiert, dass alles in Ordnung und das Gerät geschützt ist.

Durch Wischen nach rechts wird ein Überblick angezeigt, welcher Daten des letzten Scans, Status zu Updates und der Lizensierung zeigt.

Durch Wischen von unten nach oben werden alle verfügbaren Funktionen eingeblendet.



Scan

Diese Komponente von Kaspersky Internet Security ermöglicht es dem Nutzer das Gerät nach Schadsoftware zu scannen. Hierfür werden drei unterschiedliche Modi angeboten: Quick Scan untersucht alle installierten Dateien, Full Scan das ganze Gerät und mit einem Folder Scan können spezifische Ordner gescannt werden.

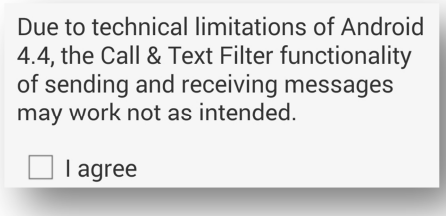
Browser

Kaspersky bietet für den Schutz des Users während des Surfens im Internet einen Browserschutz an. Kaspersky gibt an gegen Malware und Phishing Attacken zu schützen. Hierfür schlägt das Programm vor, Google Chrome als Standardbrowser einzusetzen. Wir konnten keine Informationen finden, welche Browser unterstützt werden. Ein weiterer Bestandteil der Webprotection schützt den Nutzer vor Phishinglinks, welche per SMS an den Nutzer gesendet werden.

Diese Komponente hat in unserem Test gut funktioniert. Es wird eine Meldung eingeblendet, dass der Zugriff auf die Seite blockiert wurde.

Call & Text Filter

Beim ersten Start der Komponente erscheint ein Popup, welches darauf hinweist, dass es aufgrund technischer Einschränkungen von Android Version 4.4 zu Problemen beim Senden und Empfangen von Nachrichten kommen kann. Nur durch Zustimmung des Dialogs kann fortgesetzt werden.


Due to technical limitations of Android 4.4, the Call & Text Filter functionality of sending and receiving messages may work not as intended.
I agree

Anschließend wird ein schlicht gehaltener Dialog angezeigt. Mit Black- und Whitelists können Nummern entweder geblockt oder explizit erlaubt werden.

Kaspersky bietet verschiedene Modi für die Blockierung: *Blocked Contacts* blockiert alle Nummern, welche auf der Blacklist stehen. *Allowed Contacts* erlaubt nur SMS und Anrufe von Nummern, welche auf der Whitelist stehen, alle anderen werden abgewiesen. Im *Standard Modus* werden Nummern aus der Blacklist abgewiesen und Nummern aus der Whitelist zugelassen. Für solche, die auf keiner der beiden Listen stehen, wird eine Dialogbox angezeigt um den Nutzer entscheiden zu lassen, wie mit dem Anrufer weiter verfahren werden soll.

Für die Blacklist kann bestimmt werden, ob nur SMS, nur Anrufe, oder beides abgewiesen werden soll. Nummern können entweder manuell eingegeben, oder aus dem Anruf- und SMS Verlauf importiert werden.

Das Blockieren der Telefonanrufe hat in unserem Test ausgesprochen gut funktioniert. Bei den SMS kam es jedoch zu Problemen, wie auch schon von Kaspersky angekündigt. Hier konnten wir nicht nur feststellen, dass die SMS nicht blockiert wurden, sondern dass Nachrichten, die eigentlich nicht gefiltert werden hätten sollen, nicht den Weg in den Posteingang gefunden haben. Ein derartiges Verhalten kann sogar noch unangenehmer sein, als wenn diese Funktion gar nicht erst funktioniert hätte. Auf unserem alternativen Testgerät mit Android 4.1.2 hat auch die SMS Blockfunktion gut funktioniert.

Privacy Protection

Beim Aktivieren dieser Funktion warnt Kaspersky wieder, dass es beim Empfangen und Senden von Nachrichten Probleme mit der aktuellen Android Version 4.4 geben kann.

Im folgenden Schritt muss der Nutzer eine Lizenzvereinbarung akzeptieren, die vor allem die Nutzung der Daten betrifft. Anschließend muss Kaspersky als Geräteadministrator eingetragen werden. Hier meldet die Applikation, dass sie gerne der einzige Geräteadministrator auf dem Gerät wäre. Somit wird gefordert, dass Google Play Services von den Geräteadminstratoren ausgetragen werden. Dieser Schritt kann jedoch auch übersprungen werden. Im Anschluss muss ein Kaspersky Account registriert werden. Hierfür muss die Emailadresse und ein Passwort (8 Zeichen, Kombination aus Kleinbuchstaben, Großbuchstaben und Zahlen) eingegeben werden. Im Anschluss wird der Nutzer aufgefordert einen Sicherheitscode (vier bis 16 Stellen) zu definieren. Kaspersky empfiehlt diesen aufzuschreiben und sicher abzulegen, ebenso wie die Verwendung von Keys die eine Länge von mindestens sieben Ziffern haben.

Nach der Aktivierung wird das Einstellungsmenü für Privacy Protection angezeigt. Dieses Modul erlaubt das Verstecken von Kontakten im Adressbuch, sowie SMS und Anruflogs. Die zu versteckenden Kontakte können über ein einfaches Menü definiert werden.

In unseren Tests hat diese Komponente insgesamt sehr gut funktioniert. Die Kontakte wurden ausgeblendet, ebenso wie die Anruflogs. Die SMS waren jedoch noch im Posteingang. Dort waren immerhin die Namen des Kontakts nicht mehr sichtbar (weil nicht mehr im Telefonbuch vorhanden). Für das Deaktivieren der Privacy Protection ist die Eingabe eines PIN Codes erforderlich. In den

Einstellungen kann eingestellt werden, dass nach einer gewissen Zeit die Kontakte automatisch wieder versteckt werden sollen.

Anti-Theft

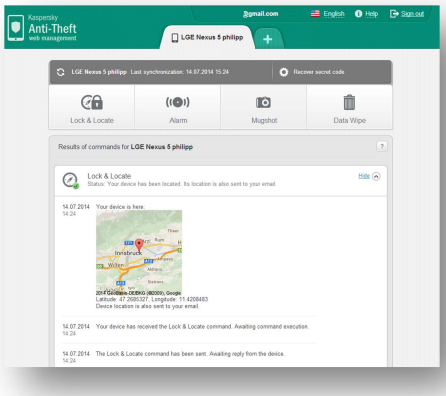
Der Diebstahlschutz von Kaspersky wird über ein Webinsterface (http://anti-theft.kaspersky.com) gesteuert. Zusätzlich sind SMS Kommandos verfügbar, welche wir in unserem Test jedoch nur schwer finden konnten.

Lock and Locate

SMS Kommando: Find: <PIN>

Diese Funktion ermöglicht das Orten und Sperren eines verlorengegangenen oder gestohlenen Geräts. Nach der Ortung wird die Position in einer Google Maps Karte eingetragen. Gleichzeitig wird das Gerät mit dem androidinternen Sperrbildschirm gesperrt. Dieser ist im Allgemeinen sehr sicher und wir konnten ihn nicht umgehen. Sollte der Nutzer den PIN vergessen haben, so kann er einen Recovery Code im Webinterface abrufen. Dieser ist 16 Stellen lang und lässt anschließend den originalen PIN im Klartext erscheinen. Gut gefallen hat uns auch, dass es möglich ist eine personalisierte Nachricht am Sperrbildschirm anzeigen zu lassen. Hier könnten etwa Kontaktinformationen eingetragen werden.

Bei der Verwendung von SMS Kommandos erhält der Absender ein SMS mit den Koordinaten des Geräts. Dies ist jedoch sehr unhandlich. Hier wäre es wohl sinnvoller direkt Links zu Kartendiensten zu versenden.



Alarm

SMS Kommando: Alarm: <PIN>

Diese Funktion sperrt das Gerät und lässt einen Alarmton ertönen. Dies kann beim Wiederfinden eines verlegten Geräts hilfreich sein. Auch hier kann die Nachricht auf dem Sperrbildschirm definiert werden.

Mugshot

Diese Funktion erstellt Fotos des Diebs mit der Frontkamera. Diese werden anschließend im Webinterface der Diebstahlsicherung angezeigt. So wird es dem Nutzer ermöglicht einen Dieb zu identifizieren. Dieses Kommando ist nur für das Webinterface verfügbar, nicht für SMS.

Wipe

SMS Kommando: Wipe: <PIN>

Die Wipe Funktion löscht persönliche Daten vom Gerät des Nutzers. So kann verhindert werden, dass möglicherweise vertrauliche Informationen in die Hände Unbefugter gelangen.

Kaspersky bietet zwei unterschiedliche Arten von Wipes an. Bei der ersten Variante werden nur die persönlichen Daten vom Gerät gelöscht. Dazu gehören Kontakte, Nachrichten, Kalender und Google Account. Der Diebstahlschutz bleibt hierbei aktiv. In unseren Tests wurden alle Daten gelöscht, jedoch nicht der Browserverlauf und die Favoriten.

Bei der zweiten Variante wird das Gerät zusätzlich aus Werkseinstellungen zurückgesetzt (***SMS Kommando: fullreset: <PIN>)***. Dies hat zur Folge, dass der Diebstahlschutz anschließend nicht mehr verfügbar ist. In diesem Fall wurden alle Daten gelöscht, jedoch ist in diesem Fall der Diebstahlschutz nicht mehr aktiv. Die Daten auf der externen SD Karte konnten mit gängigen Freewareprogrammen wiederhergestellt werden.

SIM Watch

Die SIM Watch Funktion erkennt, wenn eine andere SIM Karte eingelegt wurde, zum

Beispiel die eine Diebes. In diesem Fall wird das Gerät gesperrt. Zusätzlich kann eine Nummer und eine Emailadresse eingetragen werden, welche im Falle eines SIM Wechsels kontaktiert wird.
Die Funktion hat in unserem Test sehr gut funktioniert. Das Gerät wurde gesperrt, Benachrichtigungen per SMS und Email wurden versandt.

Updates

Updates können durch einfaches Tippen auf dem Startbildschirm manuell gestartet werden. Zusätzlich sind automatische Aktualisierungen, welche täglich oder wöchentlich ohne weiteres Zutun des Nutzers durchgeführt werden können. Zusätzlich kann der gewünschte Zeitpunkt für den Vorgang festgelegt werden.

Hilfe

Kaspersky bietet eine wirklich umfangreiche Hilfe an. Diese sollte ausreichend Informationen bieten um etwaige Probleme zu lösen. In den meisten Dialogen ist in der rechten oberen Ecke eine sehr (!) kleine Fragezeichenbox, welche den Nutzer direkt zu der entsprechenden Hilfeseite leitet.

Deinstallation

Um Kaspersky Internet Security zu deinstallieren muss die Applikation aus der Liste der Geräteadministratoren ausgetragen werden. Hierbei ist eine Passworteingabe erforderlich. Dies ist auch sinnvoll, ansonsten könnte ein Dieb das Produkt einfach vom Gerät deinstallieren. Für noch komfortablere Deinstallation wird ein Assistent angeboten, welcher den Schritt des Deaktivierens des Geräteadministrators übernimmt.

Lizenz

Kaspersky Internet Security kann mit Basisfunktionen kostenlos genutzt werden. Für einen erweiterten Funktionsumfang ist ein Premium Paket notwendig, welches für 10,95€ pro Jahr erhältlich ist. Dieses umfasst Echtzeitvirenschutz, Webprotection, Privacy Protection und Text Antiphishing.

Fazit

Kaspersky liefert auch im diesjährigen Test ein gutes Sicherheitsprodukt für Android. Sinnvolle Funktionen wie SMS Antiphishing, Privacy Protection und Diebstahlschutz haben im Test insgesamt eine gute Figur gemacht. Dass SMS, welche nicht gefiltert werden sollten, offensichtlich trotzdem geblockt werden, muss Kaspersky dringend untersuchen und beheben.

Kingsoft Mobile Security

Kingsoft Mobile Security ist ein kostenloses Sicherheitsprodukt, welches optisch so simpel wie möglich gehalten wurde. Der Startbildschirm ist in zwei Teile gesplittet. Auf der ersten Seite wird sowohl ein „Super Energy Saver“, als auch ein „App Behavior Manager“ angeboten. Durch Wischen nach rechts gelangt der Nutzer zum Hauptmenü. Dort wird Behaviour Monitor, ein Blocker von Störanrufen und Spam SMS, ein Schutz bei Bezahlvorgängen, sowie ein sicherer QR Code Scanner angeboten.

Bei eingehenden und ausgehenden Anrufen innerhalb Chinas zeigt Kingsoft die Provinz, Gemeinde oder Region des Gesprächspartners an.

Installation

Wir haben die Applikation bei Baidu heruntergeladen, welche als „offizielle Version“ markiert wurde. Das Akzeptieren der Lizenzvereinbarungen ist standardmäßig aktiviert.

Starten des Programms

Beim ersten Start des Programms wird ein sehr simples Menü angezeigt, welches aus lediglich zwei Schaltflächen besteht. Dabei handelt es sich zum einen um den „Super Energy Saver“, und um den „App Behavior Manager“ zum anderen.

Complete Checkup

Aus der Mitte des Startbildschirms werden die Ergebnisse des letzten „Complete Checkups“ eingeblendet. Die Kingsoft Applikation prüft das System nach Lecks, Viren, Trojanern, energieverschwendenden Applikationen, aggressiver Werbung und Problemen betreffend der Privatsphäre. Wird ein Problem erkannt, so kann dieses durch ein einziges Tippen behoben werden.

In unserem Test hat Kingsoft ein Leck im Betriebssystem entdeckt und empfohlen dieses sofort zu beheben. Zudem wurde die Applikation „Amazing Alex“ als schadhaft erkannt, da es die Telefonnummer des Geräts auslesen kann, was offenbar zu SMS Spam führen kann.

In der aktuellen Version der Applikation wurde die AV Komponente in die „Complete Checkup“ Funktion integriert.

Super Energy Saver

Diese Registerkarte zeigt die voraussichtlich verbleibende Batterielaufzeit an. Durch Änderung der Einstellungen laufender Applikationen kann der Nutzer die Batterielaufzeit verlängern.

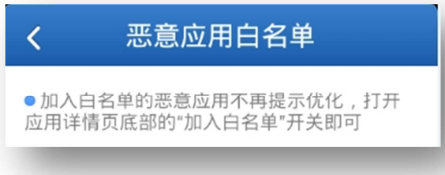
Main Menu

Der Nachfolgende Screenshot zeigt das Hauptmenü. Über den ersten Eintrag erreicht der Nutzer den „App behaviour log“. Dort können laufende Apps überwacht werden und geblocktes Verhalten angezeigt werden.

In den Einstellungen kann der Nutzer jeweils folgende Optionen aktivieren und deaktivieren: Installation von Apps, Energieverbrauch von Apps, der Umgang mit Werbeframeworks, der Umgang mit privaten Daten, sowie der Umgang mit schadhaften URLs. Zudem kann eingestellt werden, ob die Cloud verwendet werden soll oder nicht.

Bezüglich der Updates kann eingestellt werden, ob diese nur bei aktiver WLAN Verbindung durchgeführt werden sollen, oder immer. Außerdem kann auch das Senden von Feedback an Kingsoft nur auf das WLAN Netzwerk beschränkt sein. Die Heuristik Engine befindet sich nach wie vor im Beta-Stadium. Nach der Aktivierung wird der Nutzer darauf aufmerksam gemacht, dass dies die Geschwindigkeit erheblich bremsen kann. Zudem wird sehr offensiv darauf aufmerksam gemacht, dass die Heuristikengine im Normalfall nicht eingeschaltet werden muss.

Wir waren sehr verwundert über eine Whitelistingfunktion, welche es erlaubt Schadsoftware grundsätzlich zu erlaubten. Diese Option kann in den Einstellungen gefunden werden. In unseren Augen macht es keinen Sinn Schadsoftware grundsätzlich zuzulassen. Sollte Kingsoft mit dieser Funktion eine andere Idee verfolgen, so sollte dies in der Beschreibung entsprechend erklärt werden.



App Behaviour Manager (ABM)

Auf dieser Registerkarte werden alle installierten Applikationen gelistet. Auf Unterseiten werden die Apps in Unterkategorien unterteilt, wie etwa solche, die viel Batterie verbrauchen, Werbenetzwerke integriert haben, oder sehr viele Berechtigungen erfordern (wie etwa das Auslesen von SMS- und Anruflogs).

Disturbance Blocker

Da Spam SMS und unerwünschte Werbeanrufe in China nach wie vor ein großes Problem darstellen wird diese Funktion von Nutzern sehr geschätzt. Viele sind auch bereit sich an Verbesserungen zu beteiligen, wie etwa dem Melden von Telefonnummern von Werbeanrufen. In unserem Test wurden mehrere derartige Anrufe korrekt erkannt und blockiert. Jedoch wurde eine derartige Telefonnummer nicht als Werbenummer erkannt, wenn die Vorwahl nicht eingegeben und die Nummer anschließend angerufen wird.

Payment Guard

Wie auch andere Chinesische Hersteller hat auch Kingsoft eine „Payment Guard“ Funktion implementiert. Diese wurde entwickelt um bei Banktransaktionen sicher SMS empfangen zu können, zum Beispiel beim Empfang von SMS Tans. Diese können entweder innerhalb der App gespeichert, oder nach Verwendung sofort gelöscht werden.

Update, Help & Uninstallation

Updates werden automatisch durchgeführt.

Außer der Hilfe beim Payment Guard ist sämtliche angebotene Hilfe verständlich ausgeführt. Wir konnten jedoch keine Online-Hilfe finden. Nutzer können direkt Feedback zum Produkt an den Hersteller übertragen.

Für die Deinstallation ist kein Passwort erforderlich, was jedoch aufgrund des Fehlens einer Diebstahlsicherung kein Problem darstellt.

Lizenz

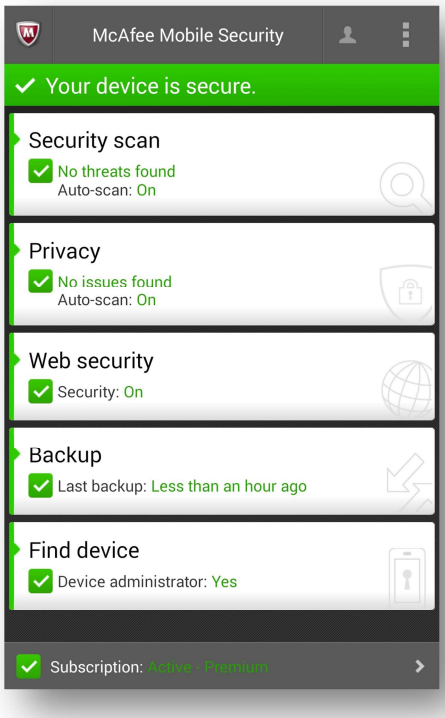
Kingsoft ist kostenlos verfügbar.

Fazit

Kingsoft Mobile Security ist ein Sicherheitsprodukt, welches einfach zu bedienen ist. Bedauerlicherweise ist immer noch kein Diebstahlschutz integriert worden. Wir empfehlen die Implementierung einer derartigen Komponente, da die privaten Daten des Nutzers geschützt werden müssen und die Gefahr eines Diebstahls nicht zu unterschätzen ist. Die Integrierung der AV Komponente in die Checkupfunktion macht Sinn und macht die Anwendung in der Verwendung noch einfacher.

McAfee Mobile Security

McAfee Mobile Security bietet alle wichtigen Funktionen, die von einem Securityprodukt auf Android erwartet werden können. Die kostenlose Version bietet einen großen Funktionsumfang, lediglich für die Backupfunktion von Mediendateien ist eine Premiumlizenz erforderlich.



Installation

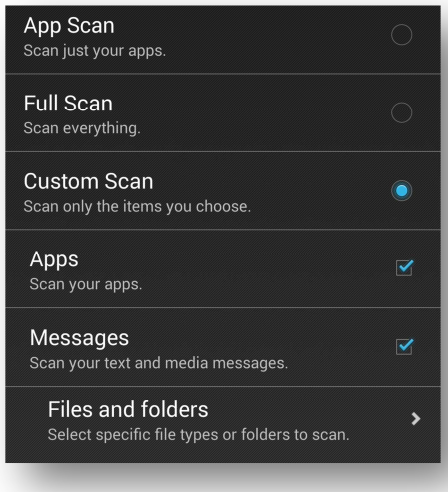
McAfee Mobile Security wurde aus dem Google Play Store bezogen und installiert. Im ersten Schritt müssen die Lizenzbedingungen akzeptiert werden. Anschließend ist das Setup beendet.

Starten des Programms

Beim ersten Start des Programms werden ein initialer Malwarescan, sowie ein Privacyscan durchgeführt. Anschließend wird der Startbildschirm angezeigt, wo signalisiert wird, dass noch kein Backup eingerichtet wurde. Alle anderen Komponenten erscheinen grün, was bedeutet, dass alles in Ordnung ist. Am oberen Bildschirmrand erschien in unserem Test eine orange „2“. Durch Antippen zeigt McAfee Mobile Security unter dem Stichwort „wichtig“ an, dass wir einen Lockscreen aktivieren sollen, sowie „McAfee Mobile Innovations“ installieren sollen. Hierbei handelt es sich um eine Applikation, die es dem Nutzer erlaubt andere McAfee Programme, welche sich noch im Betastadium befinden, zu testen. Nette Sache, jedoch in unseren Augen zu Unrecht als „wichtige“ Benachrichtigung angeführt, obwohl uns McAfee in diesem Punkt widerspricht.

Security Scan

Diese Komponente erlaubt es dem Nutzer sein Smartphone auf Schadsoftware zu überprüfen. Der Scan kann auch zeitgesteuert automatisch gestartet werden. Hierfür können die Intervalle „täglich“ und „wöchentlich“ gewählt werden. In den Optionen kann der Nutzer den Umfang eines Scans einstellen. Standardmäßig ist der „Full Scan“ aktiv, kann jedoch auf „App Scan“ und „Custom Scan“ umgestellt werden.

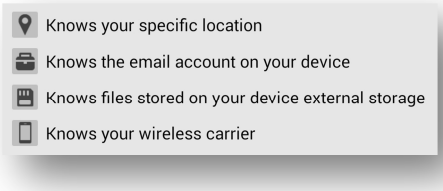


Der „App Scan“ überprüft nur die installierten Anwendungen, für den „Custom Scan“ kann festgelegt werden ob Apps, Nachrichten und bestimmte Ordner geprüft werden sollen.

App Privacy

Die App Privacy Funktion erlaubt es dem Nutzer installierte Applikationen auf mögliche Verletzungen der Privatsphäre zu prüfen. Alle Apps werden in einer List angeführt und in verschiedene Gefahrenklassen eingeteilt. In

unserem Test waren nur „Medium“ und „Low“ vorhanden. Schwerwiegende Fälle von Verletzungen werden in eine eigene Liste „Noticable Apps“ eigetragen. Durch Antippen werden Details zur App gegeben und Gründe für die Beanstandung angeführt, wie zum Beispiel, dass die Applikation die Möglichkeit besitzt das Gerät zu orten. Aus diesem Menü kann die Applikation anschließend direkt deinstalliert werden.


Knows your specific location
Knows the email account on your device
Knows files stored on your device external storage
Knows your wireless carrier

In den Einstellungen kann aktiviert werden, ob Privacy Scans automatisch durchgeführt werden sollen.

Privacy Control

Die Privacy Control ermöglicht es dem Nutzer persönliche Daten zu schützen, sowie Störenfriede abzuweisen. Nachfolgende Funktionen werden hierfür angeboten.

Lock Apps

Die Lock Apps Funktion ermöglicht es dem Nutzer installiere Applikationen mit einem PIN zu sperren. Dies muss vor dem Start einer App eingegeben werden. Anderenfalls ist die Verwendung nicht möglich. In der Konfiguration kann der Nutzer aus einer Liste aller Anwendungen auswählen welche geschützt werden sollen. In unseren Tests funktionierte der App Lock wie erwartet. Es war uns nicht möglich eine gesperrte Applikation ohne PIN zu verwenden.

Set Profile

McAfee Mobile Security ermöglicht es dem Nutzer aus einem von vier Profilen zu wählen (Keine Einschränkung, Büro, Kinder, Gast). Für jedes dieser Profile kann gewählt werden, welche Applikationen verfügbar sein sollen. Um andere Apps auszuschließen hat McAfee einen eigenen Launcher implementiert, welcher nur die erlaubten Apps anzeigt. Beim Versuch zum originalen Startbildschirm zurückzuwechseln um Zugriff auf alle installierten Apps zu erhalten ist die Eingabe des Pins erforderlich.

In unserem Test hat die Komponente gut funktioniert. Es war uns zwar möglich kurz auf den originalen Startbildschirm zu gelangen und durch diesen zu navigieren, für die aktive Nutzung geblockter Apps hat die Zeit bis zur Anzeige der PIN-Eingabe jedoch nicht gereicht.

Block Calls

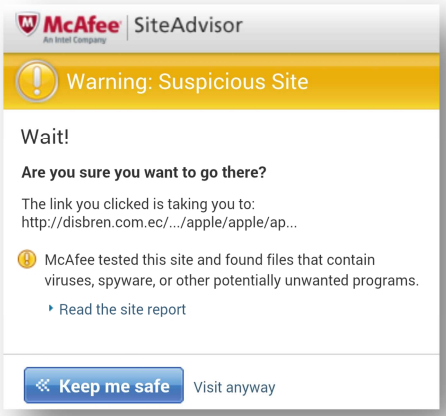
Um unerwünschte Anrufe abzuweisen liefert McAfee die Funktion „Block Calls“ mit. Diese arbeitet sowohl mit Black- als auch mit Whitelists. In den Einstellungen kann festgelegt werden wie die Filterfunktion für eigehende-, ausgehende- und Roaminganrufe arbeiten soll. Für jede der drei Arten kann der Nutzer definieren ob alle erlaubt, nur Anrufe aus der Whitelist erlaubt, Anrufe aus der Blacklist blockiert, oder überhaupt alle Anrufe blockiert werden sollen. Zusätzlich kann der Nutzer entscheiden ob Anrufer mit unterdrückter Nummer blockiert werden sollen, oder nicht.

Das Blockieren von SMS wird für Android 4.4 und höher nicht unterstützt. In unserem Test haben wir feststellen können, dass beim Empfang eines SMS von einer blockierten Nummer ein Popup „SMS from … blocked“ eingeblendet wird. Die Funktion scheint demnach implementiert zu sein, jedoch nur im Menü ausgeblendet zu sein. Auf die Deaktivierung des Popups wurde vergessen.

Auf dem alternativen Testgerät mit Android 4.1.2 war die Funktion jedoch schon verfügbar und hat funktioniert. Sie erlaubt das Blockieren von SMS wie auch beim Filter für Telefonanrufe auch, sowie das Filtern von SMS, welche frei definierbare Schlüsselwörter enthalten.

Web Security

Die Web Security schützt den Nutzer während dem Surfen im Internet vor schadhaften Webseiten. Dies hat in unserem Kurztest auch verlässlich funktioniert.


McAfee SiteAdvisor
Warning: Suspicious Site
Wait!
Are you sure you want to go there?
The link you clicked is taking you to:
http://disbren.com.ec/.../apple/apple/ap...
McAfee tested this site and found files that contain viruses, spyware, or other potentially unwanted programs.
Read the site report
Keep me safe
Visit anyway

Zusätzlich bietet McAfee eine Wi-Fi Security. Diese warnt den Nutzer, wenn sich dieser mit einem unsicheren WLAN-Netzwerk verbindet.

Backup

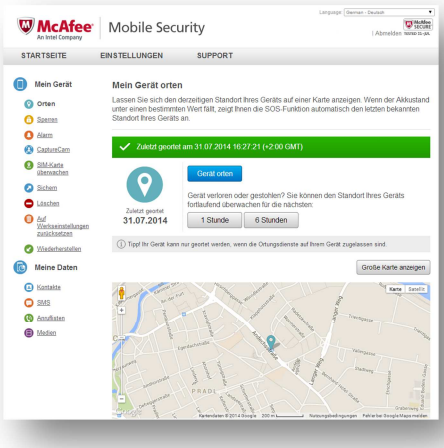
Für den Fall, dass das Gerät des Nutzers entweder verlorengegangen oder kaputt ist hat McAfee eine Backupfunktion implementiert. Diese ermöglicht die Sicherung von Textnachrichten, Anruflogs, Kontakten sowie Mediendateien wie Videos und Bilder auf Server von McAfee. Diese sind anschließend im Webinterface sichtbar und downloadbar. Backups können entweder manuell angestoßen oder von McAfee automatisch durchgeführt werden. Hierfür lässt sich kein Intervall definieren, jedoch kann eingestellt werden, dass die Synchronisation nur über WiFi erfolgen darf. Außerdem lässt sich die Sicherung aus dem Webinterface heraus für Kontakte, SMS und Anruflogs anstoßen. Dies kann sinnvoll sein, wenn das Gerät verloren wurde. In einem derartigen Fall kann der Nutzer wenigstens noch seine Daten sichern.

Kontakte und SMS können direkt vom Smartphone aus wiederhergestellt werden. In unserem Test war nur das Zurücksichern von Kontakten möglich. In der Hilfe haben wir die Information gefunden, dass die Wiederherstellung von SMS auf Android 4.4 nicht unterstützt wird. Auf unserem alternativen Testgerät mit Android 4.1.2 hat die Funktion einwandfrei funktioniert.

Eine weitere Funktion der Backupkomponente ist das sichere Löschen von Daten auf dem Smartphone. Es können Kontakte, Anruflogs, die SD Karte, Photos und Videos gelöscht werden. Dies kann zum Beispiel sinnvoll sein, wenn der Nutzer sein Gerät verkaufen möchte und zuvor das Gerät von persönlichen Daten bereinigen möchte.

Find Device

Unter dem Menüpunkt „Find Device“ findet der Nutzer den Diebstahlschutz. Dieser wird entweder über ein Webinterface (https://www.mcafeemobilesecurity.com) oder über SMS Kommandos gesteuert.



Orten

SMS Kommando: Secure locate <PIN>

Diese Funktion ortet ein verlorengegangenes oder gestohlenes Gerät. Anschließend wird die Position in einer Karte von Google Maps dargestellt. Im Falle einer Ortung per SMS

wird dem Sender des Befehls ein Link auf eine Webseite von McAfee gesendet, wo eine Google Maps Karte eingebettet ist. Gefallen hat uns, dass es möglich ist den Bewegungsverlauf des Geräts aufzunehmen. Hierfür bietet McAfee Intervalle von einer und sechs Stunden an in denen das Gerät automatisch geortet wird.

Sperren

SMS Kommando: Secure lock <PIN>

Diese Funktion sperrt das Gerät aus der Ferne und verhindert somit den Zugriff von Unbefugten. Im Webinterface kann zudem ein benutzerdefinierter Text eingestellt werden, welcher im Falle einer Sperre erscheint. Dies kann sinnvoll sein, wenn man einem Finder die Möglichkeit bieten möchte um das Gerät zurückzugeben. Dieser kann auch per SMS geändert werden, indem er einfach an den SMS Befehl angehängt wird. Die Sperren-Funktion kann mit der Alarm-Funktion kombiniert werden, welche im folgenden Abschnitt näher erklärt wird.

In unserem Test hat diese Funktion ausgesprochen gut funktioniert. Es war uns nicht möglich auf den Homescreen, die Notification Bar oder andere Ansichten zuzugreifen. Außerdem war es zu jeder Zeit möglich einen Notruf abzusetzen.

Alarm

SMS Kommando: Secure alarm <PIN>

Dieses Kommando bewirkt das Ertönen einer schrillen Sirene. Dies kann dem Wiederfinden eines verlorenen Smartphones dienen. Außerdem kann die Funktion in Kombination mit der Sperren-Funktion eventuell einen Dieb dazu bewegen das Gerät liegen zu lassen.

CaptureCam

SMS Kommando: Secure message <PIN>

Die CaptureCam nimmt mit der Frontkamera des Smartphones ein Foto auf, welches dem Nutzer anschließend per Mail zugesandt wird. So kann er feststellen wer gerade das Gerät in Verwendung hat. McAfee hat eine raffinierte Methode entwickelt, die sicherstellt, dass das Gesicht des Diebs fotografiert wird und nicht etwa die Innenseite der Hosentasche.

Die Basisfunktionalität ist zufriedenstellend, jedoch verstehen wir nicht, warum die aufgenommenen Fotos nicht im Webinterface eingesehen werden können, wie jeglicher andere Content auch. Ein weiterer, schwerwiegenderer Kritikpunkt ist, dass im Falle einer Bildschirmsperre (die vermutlich als erste Aktion nach einem Verlust oder Diebstahl gesetzt wird) die „clevere Methode“ um das Gesicht des Diebes zu erfassen nicht funktioniert. Somit kann kein Bild vom Dieb mehr aufgenommen werden. In diesem Fall muss sich der Bestohlene entscheiden: Bildschirmsperre oder CaptureCam.

Löchen

SMS Kommando: Secure wipe <PIN>

Dieser Befehl löscht persönliche Daten des Nutzers vom Smartphone. Hierbei wird das Gerät nicht auf Werkseinstellungen zurückgesetzt, was den Vorteil bringt, dass der Diebstahlschutz weiterhin aktiv bleibt. Der Nutzer kann auswählen welche Daten genau gelöscht werden sollen, wie etwa Kontakte, SMS, SD Karte, Fotos und Videos. In unserem Test wurden alle Daten, die angeführt wurden, gelöscht, jedoch war es möglich mit gängiger Freeware die gelöschten Dateien der externen SD Karte wiederherzustellen.

Auf Werkseinstellungen zurücksetzen

SMS Kommando: Secure reset <PIN>

Dieses Kommando löscht die persönlichen Daten vom Smartphone, wie auch schon beim Löschen-Befehl. Zusätzlich wird das Gerät auf Werkseinstellungen zurückgesetzt. Danach kann der Diebstahlschutz nicht mehr verwendet werden. Auch hier war es möglich die Dateien der externen SD Karte wiederherzustellen.

SIM-Karte überwachen

Dieses Feature sperrt das Gerät wenn eine fremde SIM Karte eingelegt wurde. Dies kann zum Beispiel der Fall sein, wenn ein Dieb seine eigene SIM Karte verwenden möchte.

Eine Benachrichtigung haben wir in unseren Tests nicht erhalten.

Updates

Updates können automatisch durchgeführt werden. In den Einstellungen kann eingestellt werden, ob dieser Vorgang täglich oder nur wöchentlich durchgeführt werden soll. Zusätzlich kann der Nutzer eine Aktualisierung manuell anstoßen.

Hilfe

McAfee bietet dem Nutzer Hilfe in mehreren Formaten. Zum einen existiert eine ausführliche Hilfe in Form einer Hilfeseite. Zum anderen kann in jeder Ansicht des Programms auf einen Infobutton getippt werden, welcher eine Schnelleinführung bietet.

Deinstallation

Dem Nutzer wird ein Deinstallationsassistent angeboten, welcher notwendige Schritte, wie die Deaktivierung des Geräteadministrators, übernimmt. Hierfür ist eine PIN-Eingabe notwendig, wodurch es einem Dieb nicht möglich ist den Diebstahlschutz einfach zu deaktivieren.

Lizenz

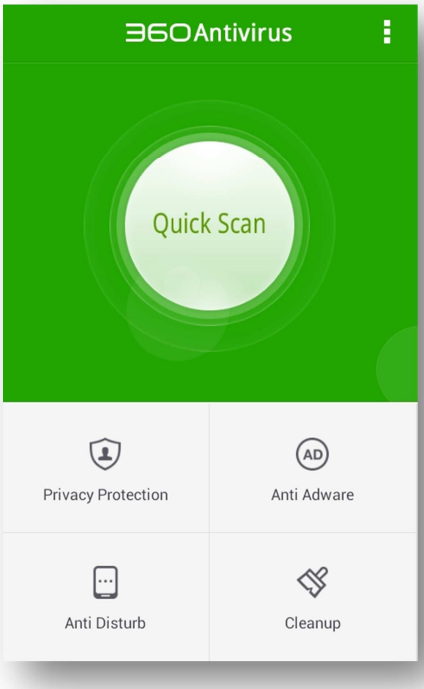
McAfee Mobile Security ist kostenlos im Google Play Store erhältlich. Für die Backupfunktion, Telefonsupport und Entfernen der Werbebanner ist eine Premiumlizenz erforderlich, welche für 2,49€ monatlich oder 29,99€ jährlich erhältlich ist.

Fazit

McAfee bietet ein solide implementiertes Sicherheitsprogramm für Android, das viele Funktion mit sich bringt. Der Diebstahlschutz ist verlässlich und kann über ein Webinterface gesteuert werden. Erfreulich ist, dass trotz free/premium Modell viele der verfügbaren Funktionen auch in der kostenlosen Version verfügbar sind.

Qihoo 360 AntiVirus

Qihoo 360 Antivirus ist ein kostenloses Antivirenprodukt, welches neben Sicherheitsfeatures wie Antivirus und Echtzeitscan auch ausgeklügelte Funktionen wie Anti-Adware bietet. Ein Diebstahlschutz fehlt jedoch. Qihoo hat uns darauf aufmerksam gemacht, dass die chinesische Version einen weit höheren Funktionsumfang bietet als die getestete englische Version.
Das erreichte Ergebnis in diesem Test ist nicht übertragbar auf die englische Produktversion die im Google playstore verfügbar ist. Qihoo hat diese Auszeichnung in ihren entsprechenden Pressemitteilungen missbraucht und daher wird diese Auszeichnung zurückgezogen.



Installation

Qihoo 360 Antivirus wurde von der Webseite des Herstellers (http://shouji.360.cn/sd/) in Form einer APK bezogen und installiert.

Im ersten Schritt werden die Lizenzvereinbarungen akzeptiert. Außerdem kann der Nutzer entscheiden, ob er am Experience Improvement Program teilnehmen möchte (Opt-Out). Im Anschluss wird der Startbildschirm eingeblendet.

Starten des Programms

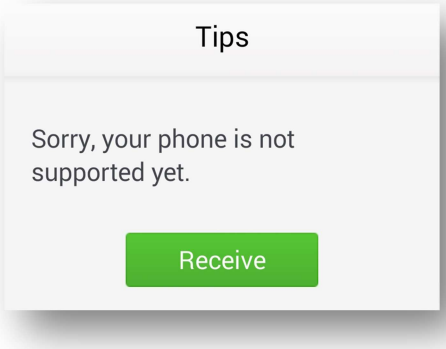
Der Startbildschirm ermöglicht durch einen großen Button das Starten eines Quickscans. Im oberen Teil des Bildschirms wird eine Meldung eingeblendet, dass der „Super-Modus“ aktiviert werden soll, um einige Funktionen zu aktivieren.

Antivirus

Der Nutzer hat die Möglichkeit zwischen einem Quickscan (Start über Button auf Homescreen) oder einem Fullscan (Start über Kontextmenü) zu wählen. Der Quickscan überprüft alle installieren Applikationen auf Schadsoftware. Beim Fullscan wird zusätzlich der Speicher miteinbezogen.
Für die Scans wird auch die Cloud von Qihoo hinzugezogen. Dieses Feature ist standardmäßig aktiviert, kann aber in den Einstellungen abgedreht werden. Zusätzlich ist ein Echtzeitscanner implementiert.

Super Mode

Der Super Mode ist für manche Funktionen wie dem Privacy Protector, Ad Blocker, Notification Blocker und Autostart Blocker erforderlich. Dies bedeutet jedoch nicht, dass das Gerät gerootet wird.



Bei der Aktivierung des Super Modus auf dem Nexus 5 schlug der Vorgang fehl mit der Meldung, dass dieses Gerät nicht unterstützt wird. Auf unserem alternativen Gerät hat die Aktivierung geklappt. Um den Supermodus auf dem Nexus 5 zu aktivieren muss das Gerät laut Qihoo gerootet sein.

Privacy Protection

Diese Komponente ermöglicht die Blockierung von bestimmten Berechtigungen, die die Applikation auf dem Android Betriebssystem besitzt. In unserem Test wird angezeigt, dass ein App optimiert werden kann. In unserem Test gab Qihoo an, dass eine Fileexplorer Applikation, welche auf unserem Gerät installiert ist, Zugriff auf das WiFi benötigt. Der Nutzer kann nun für diese Anwendung bestimmen ob dieser Zugriff blockiert, erlaubt, oder jedes Mal nachgefragt werden soll. In den Einstellungen lassen sich Logs zu vergangenen Ereignissen anzeigen.
Die Funktion hat in unserem Test auf dem alternativen Testgerät mit Android 4.1.2 gut funktioniert. Auf dem Nexus 5 mit Android 4.4.2 jedoch nicht.

Anti Adware

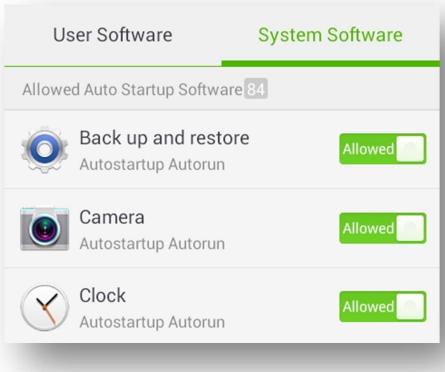
Diese Komponente entfernt Werbung aus installierten Anwendungen auf dem Gerät. Auch für diesen Teil des Produkts wird der Super-Modus vorausgesetzt. Somit ist auch die Anti-Adware Komponente nicht für unser Nexus 5 Testgerät verfügbar. Auf dem alternativen Gerät mit Android 4.1.2 hat die Komponente jedoch wirklich gut funktioniert. Apps, welche zuvor Banner eingeblendet hatten sind nun werbefrei.

Anti Disturb

Diese Komponente ermöglicht die Blockierung von Benachrichtigungen in der Notification Bar. Apps, welche zu mitteilungsbedürftig sind, kann so die Berechtigung für die Anzeige von Benachrichtigungen entzogen werden. Im „Leave Me alone“ Mode werden alle, außer sehr wichtige Benachrichtigungen, blockiert. Schön wäre gewesen, wenn sich diese Funktion noch zeitlich automatisieren ließe, so könnten etwa während den Arbeitszeiten Benachrichtigungen deaktiviert werden.
Auch diese Funktion erfordert den Supermodus. So war auch diese nicht auf dem Nexus 5 verfügbar. Auf dem alternativen Gerät funktionierte sie jedoch einwandfrei.

Block self-start apps

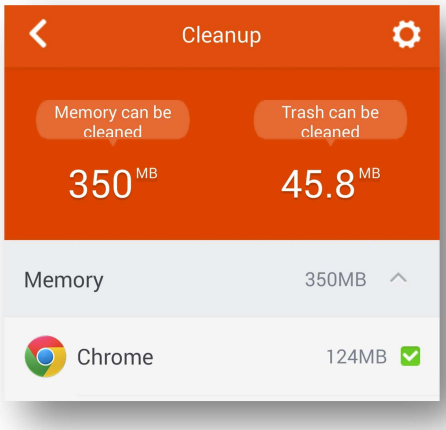
Diese Funktion hindert Apps, welche beim Systemstart des Geräts automatisch gestartet werden, an der Ausführung. Dies soll langen Systemstarts vorbeugen und verhindern, dass das Telefon langsam ist.



In den Einstellungen werden alle installierten Applikationen aufgelistet, welche bei einem Systemstart gestartet werden. Mit einem einfachen Schieberegler können diese dann an automatischen Starts gehindert werden. Dies gilt auch für Systemapplikation, hier spricht Qihoo jedoch eine Warnung aus vorsichtig zu sein.

Cleanup

Diese Funktion ermöglicht es dem Nutzer Arbeitsspeicher und Speicherplatz auf dem internen Datenträger freizugeben. In unserem Test konnten 350MB Arbeitsspeicher, sowie 4,72MB unnötige Cachedateien und 41,0MB überflüssige APK-Dateien gefunden und bereinigt werden.



Updates

Updates werden automatisch durchgeführt. Alternativ können auch manuell Aktualisierungen angestoßen werden.

Hilfe

Wir konnten keine Hilfe finden.

Deinstallation

Die Applikation kann mit dem androidinternen Anwendungsmanager deinstalliert werden. Hierfür ist keine Passworteingabe erforderlich. Dies ist auch legitim, da keine schützenswerten Funktionen wie Anti-Theft verfügbar sind.

Lizenz

Qihoo 360 Antivirus ist in vollem Funktionsumfang kostenlos verfügbar.

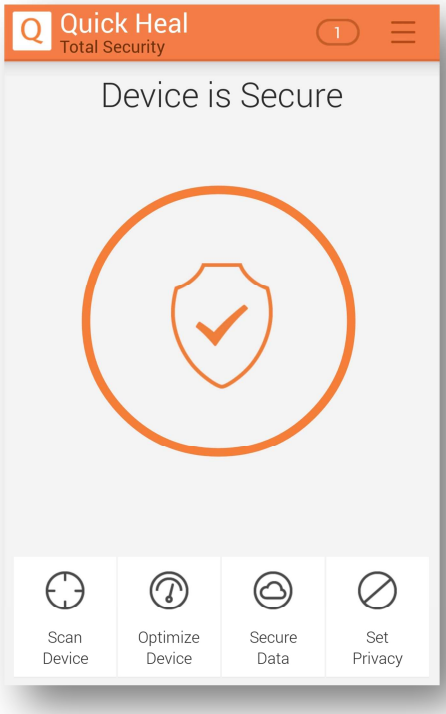
Fazit

Qihoo 360 Antivirus bietet wichtige Funktionen wie Antivirus. Innovative Features wie die Anti-Adware Komponenten haben erstaunlich gut funktioniert. Ein großes Manko ist jedoch, dass für die meisten Funktionen der Super-Mode notwendig ist. Auf unserem Testgerät, einem Nexus 5 mit Android 4.4.2 war dieser Modus nicht verfügbar, wodurch sich lediglich der Malwarescanner und die Cleanupfunktion ordentlich verwenden ließen.

Qihoo hat uns darauf aufmerksam gemacht, dass in der aktuellsten verfügbaren Version nun ein Diebstahlschutz integriert sein soll.

Quick Heal Total Security

Quick Heal bietet ein umfangreiches Sicherheitsprodukt für Android Smartphones, welches alle wichtigen Funktionen bietet, wie Diebstahlschutz, Malwareschutz, Security- und Privacy Advisor. Zusätzlich findet der Nutzer nützliche Funktionen wie Secure Data.



Installation

Die Installationsdatei wurde von der Herstellerseite bezogen und installiert. Nach dem Akzeptieren der Lizenzvereinbarung geht es an die Lizensierung. Hat der Nutzer bereits einen Lizenzschlüssel, kann er das Produkt direkt aktivieren, andernfalls einen Schlüssel bestellen.

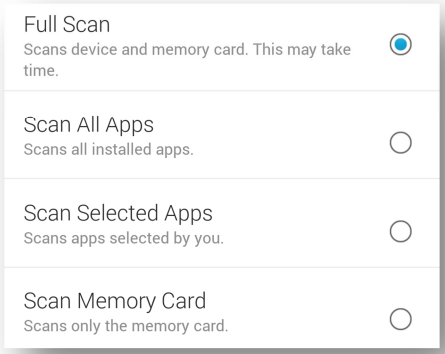
Danach wird die Diebstahlschutzkomponente konfiguriert. Hierfür muss ein 6 bis 20 stelliges Passwort definiert werden. Anschließend ist es erforderlich die Telefonnummer eines Freundes einzutragen, welcher benachrichtigt wird, wenn das Passwort vergessen wurde oder eine fremde SIM Karte eingelegt wurde. Außerdem kann an dieser Stelle ein Deinstallationsschutz gesetzt werden. Hierfür wird die Applikation als Geräteadministrator eingetragen.

Starten des Programms

Nach Abschluss des Setups wird der Startbildschirm angezeigt. Beim ersten Start wird automatisch ein Systemscan durchgeführt. Anschließend wird der Sicherheitsstatus angezeigt, welcher bei rund 95% steht, mit der Information, dass man zum Erhöhen der Sicherheit tippen solle. In einem Menü mit dem Titel „Security Measures“ werden wir darauf aufmerksam gemacht, dass der Netzwerkmonitor, die Kindersicherung, Autobackup und Personal Security nicht aktiviert wurden.

Scan Device

Diese Komponente ermöglicht das Überprüfen des Smartphones auf Schadsoftware. Hierfür kann der Nutzer zwischen einem Quickscan oder einem Custom Scan wählen. Bei der schnellen Überprüfung werden nur die installierten Applikationen geprüft. Beim Custom Scan kann der Nutzer entscheiden, ob das komplette Gerät, alle Apps, ausgewählte Apps, nur die Speicherkarte oder ausgewählte Ordner überprüft werden sollen.


Full Scan
Scans device and memory card. This may take time.
Scan All Apps
Scans all installed apps.
Scan Selected Apps
Scans apps selected by you.
Scan Memory Card
Scans only the memory card.

Zusätzlich können Scans geplant werden, welche dann in Zukunft automatisch ausgeführt werden. Dies ist sehr durchdacht implementiert worden. Der Nutzer kann mehrere Scanaufgaben anlegen. Für jede kann die Art (Full-, App-, Memorycardscan), sowie der Zeitpunkt gewählt werden. Ebenso kann die Frequenz eingestellt werden. Hierfür werden täglich, wöchentlich und monatlich angeboten. Zudem kann eingestellt werden ob

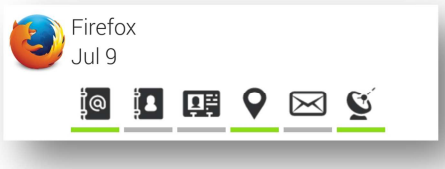
bei jedem Aufladevorgang gescannt werden soll.

Security Adviser

Der Security Adviser macht den Nutzer auf möglicherweise unsicher Einstellungen auf dem Android Smartphone aufmerksam. In unserem Test wurden fünf Einstellungen bemängelt. So wurde etwa angeführt, dass das Gerät nicht verschlüsselt wird, und dass kein Screenlock aktiviert wurde. Außerdem dass Apps aus unbekannten Quellen installiert werden können und, dass USB-Debugging aktiviert ist. Durch einfaches Klicken auf das Zahnrad neben dem Eintrag werden die Einstellungen automatisch auf die vorgeschlagene Option gesetzt.

Privacy Advisor

Dieser Teil der Anwendung überprüft installierte Applikationen auf mögliche Verletzungen der Privatsphäre. Hierfür werden alle installierten Apps aufgelistet und mit Icons signalisiert welche Berechtigungen die App hat. Durch Antippen eines Eintrags werden Details angezeigt, sowie eine kurze Beschreibung gegeben. Über einen Button am unteren Ende des Bildschirms kann die jeweilige Applikation direkt deinstalliert werden.

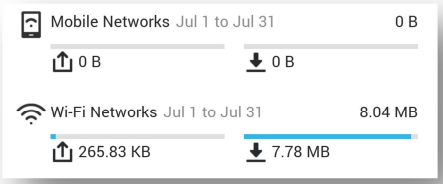


Optimize Device

In diesem Teil der Anwendung dreht sich alles um die Leistung des Geräts. In einer Übersicht lässt sich der aktuelle Zustand des Smaprtphones einsehen, so wird die aktuelle CPU Last, Akkustand und RAM-Belegung angezeigt.

Über den Menüpunkt „Kill running apps“ werden alle laufenden Applikationen angezeigt. Diese lassen sich entweder nach RAM- oder CPU-Last sortieren. Durch Auswahl mit Checkboxen kann ein oder mehrere Apps ausgewählt und geschlossen werden. In einer Whitelist können Apps eingetragen werden, welche vom „Kill“ ausgeschlossen werden sollen.

In der Network Summary wird die Datennutzung über WiFi und mobile Netzwerke in einem Graph angezeigt. Außerdem lassen sich zu jeder App Details anzeigen, wie viel die jeweilige Anwendung in den letzten 30 Tagen verbraucht hat.



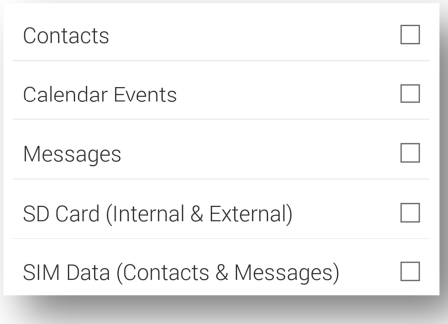
In den Einstellungen kann ein Limit für die Datennutzung aktiviert werden. Bei einer Überschreitung kann dann Quick Heal eingreifen und den Zugang zum Netzwerk unterbinden. Dies kann zum Beispiel unnötige Kosten verhindern, wenn der Nutzer nur ein begrenztes Downloadvolumen in seinem Mobilfunkvertrag inkludiert hat.

Secure Data

Mit Secure Data bietet Quick Heal einen Backupdienst in die Cloud an. Es können Kontakte, Kalendereinträge, Nachrichten, Bilder, Musik und Videos gesichert werden. Hierfür werden dem Nutzer 1024MB Speicher angeboten. Zusätzlich wird ein automatisches Update angeboten, welches die Nutzerdaten während dem Laden des Geräts automatisch sichert. Außerdem können als automatische Sicherungszyklen täglich, wöchentlich, zweiwöchentlich und monatlich gewählt werden.

Die Rücksicherung der Daten ist ebenso einfach gestaltet wie die Sicherung. Beim Restore der SMS erhalten wir die Meldung, dass Quick Heal als SMS App eingetragen werden muss, als Alternative zu Hangouts. Nach erfolgtem Abschluss wird Hangouts

jedoch wieder als Standardapplikation eingetragen.
Auch das Löschen der gesicherten Daten von den Servern von Quick Heal ist möglich.
Quick Heal bietet eine Funktion, welche das sichere Löschen von persönlichen Daten vom Smartphone ermöglicht. Hier werden Kontakte, Kalendereinträge, Nachrichten, Dateien auf internem und externem Speicher, sowie Daten auf der SIM Karte miteinbezogen. Diese Funktion kann nützlich sein, wenn man zum Beispiel das Gerät verkaufen und zuvor persönliche Daten entfernen möchte.



Set Privacy

Unter dieser Gruppe werden all jene Funktionen eingeblendet, welche der Abwehr von Gefahren und Spam dient.

Call and Message Filter

Diese Komponente dient der Blockierung von unerwünschten Anrufen und SMS. Bereits beim Start erhalten wir eine Benachrichtigung, dass das SMS Blocken auf Android 4.4 nicht verfügbar ist. Zu blockierende Nummern können entweder manuell eigegeben oder aus den Anruflogs und Kontakten importiert werden. Auch das Blockieren von Mustern in Telefonnummern ist möglich. Diese können mit „Startet mit…“ und „Endet mit…“ definiert werden. Für jeden Eintrag kann definiert werden ob nur Anrufe, nur SMS, oder beides geblockt werden soll.
Für SMS können Schlüsselwörter eingegeben werden. Sollte eine eingehende Nachricht eines der Schlüsselwörter enthalten wird diese geblockt.

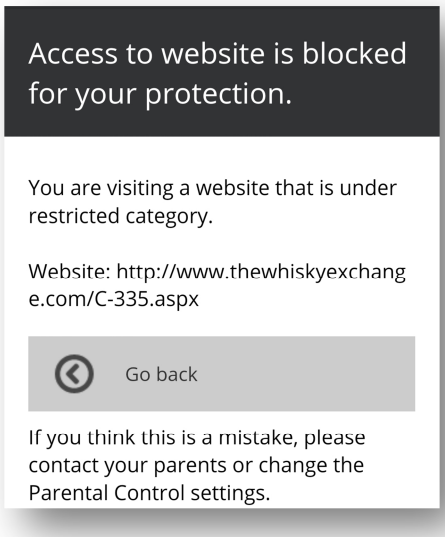
In unserem Test hat das Blockieren nicht funktioniert, wie auch bereits von Quick Heal angekündigt. Das Abweisen von unerwünschten Anrufen hat jedoch wie erwartet geklappt. Auf unserem alternativen Gerät mit Android 4.1.2 haben beide Funktionen wie erwartet funktioniert.

Privacy Protection

Diese Funktion ermöglicht das Verstecken von Kontakten, sowie deren SMS und Anruflogs. Bereits beim Start werden wir darauf hingewiesen, dass das Verstecken von SMS auf Android 4.4 nicht funktionieren wird.
Die Funktion hat insgesamt sauber funktioniert. Wie bereits angekündigt konnten die SMS nicht versteckt werden (Auf Android 4.1.2 aber schon). Immerhin wurden die Kontakte versteckt, wodurch in den SMS zumindest nur noch die Nummer ohne Name angezeigt wird.

Parental Control

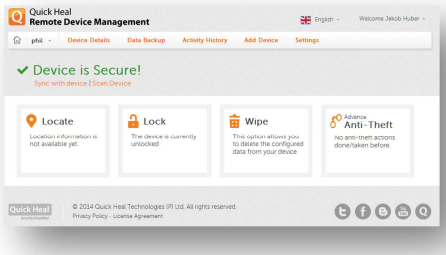
Diese Komponente schützt den Nachwuchs beim Surfen im Internet. Hierfür kommen sowohl Black- als auch Whitelists zum Einsatz. Für die Blacklist kann entweder aus einer Liste von Kategorien, wie zum Beispiel Spiele, Gewalt oder Drogen gewählt, oder eine URL manuell eingetragen werden. Auf die Whitelist können URLs gesetzt werden, welche immer zugelassen werden sollen.


Access to website is blocked for your protection.
You are visiting a website that is under restricted category.
Website: http://www.thewhiskyexchange.com/C-335.aspx
Go back
If you think this is a mistake, please contact your parents or change the Parental Control settings.

In unserem Kurztest hat die Funktion sehr gut funktioniert.

Anti-Theft

In den Einstellungen findet der Nutzer den Diebstahlschutz. Für die Steuerung werden SMS und ein Webinterface (https://mydevice.quickheal.com) angeboten.



Auf letztgenanntes macht Quick Heal nicht aufmerksam, wir mussten erst danach suchen. Für die Aktivierung wird ein „OTP – One Time Password" zugeschickt, welches der Zuordnung des Geräts dient.

Locate

SMS-Kommando: TRACE <Password>

Diese Funktion ortet das Smartphone des Nutzers und stellt die Position auf einer Karte von Google Maps dar. Es ist möglich das Gerät kontinuierlich zu orten, also den Bewegungsverlauf nachzuverfolgen.

Beim Absetzen des Befehls mit SMS Kommando erhält der Sender eine Antwort mit einem Link zu Quick Heal, wo eine Google Maps Karte eingebettet ist. Zusätzlich werden noch die Koordinaten übertragen.

Lock

SMS-Kommando: BLOCK <Password>

Die Lockfunktion sperrt das Gerät des Nutzers mit einem Sperrbildschirm. Dieser war in unserem Test sehr verlässlich und konnte nicht umgangen werden. Außerdem konnte zu jedem Zeitpunkt ein Notruf abgesetzt werden. Zudem wird der der vertrauenswürdige Kontakt angegeben, welcher direkt angerufen werden kann. Das Gerät kann entweder per Passwort oder über das Webinterface entsperrt werden.

Wipe

SMS-Kommando: WIPE <Password>

Diese Funktion löscht persönliche Daten vom Gerät des Nutzers. Auf unserem Nexus 5 wurden alle Daten gelöscht. Hierbei wird das Gerät nicht auf Werkseinstellungen zurückgesetzt. Dies hat den Vorteil dass der Diebstahlschutz aktiv bleibt.

Auf unserem alternativen Testgerät mit Android 4.1.2 wurden auch die Dateien auf der externen SD Karte gelöscht. Hier wurde der Aufwand betrieben die SD Karte zu überschreiben, weshalb der Wipe einige Stunden in Anspruch nahm. Gebracht hat es jedoch nichts – wir konnten mit gängiger Freeware die Daten wiederherstellen.

Dial Call

SMS-Kommando: CALL <Password>

Dieses Kommando bewirkt, dass der Absender des SMS Kommandos vom verlorengegangenen oder gestohlenen Handy zurückgerufen wird.

Pick up Call

SMS-Kommando: PICKUP <Password>

Dieses SMS Kommando bewirkt, dass der nächste eingehende Anruf automatisch angenommen wird. Dies hat im Vergleich zur „Dial Call" Funktion auch funktioniert, wenn das Guthaben einer Prepaid SIM Karte aufgebraucht ist.

Record Audio

SMS-Kommando: AUDIO <Password>

Nach Absetzen des SMS Kommandos werden für eine Minute lang alle Umgebungsgeräusche aufgezeichnet. Die Audiodatei ist anschließend im Webinterface im 3gp Format verfügbar.

Record Video

SMS-Kommando: VIDEO <Password>

Nach Absetzen des SMS Kommandos werden für eine Minute lang alle Umgebungsgeräusche und ein Video mit der Frontkamera aufgezeichnet. Die Videodatei ist anschließend im Webinterface im 3gp Format verfügbar. In unserem Test war auf dem Video

kaum etwas erkennbar. Die Auflösung war sehr niedrig und voller Artefakte.

Ring

SMS-Kommando: RING <Password>

Dieser Befehl lässt auf dem Smartphone eine Sirene in Form eines Rock Songs ertönen. Dies kann zum Beispiel sinnvoll sein, wenn der Nutzer sein Handy verlegt hat. Das Gerät wird hierbei nicht gesperrt.

SIM Change

Diese Funktion benachrichtigt den Nutzer per SMS wenn eine fremde SIM Karte in sein Gerät eingelegt wird. Zusätzlich wird das Smartphone gesperrt.

Updates

Updates können manuell ausgeführt werden. Informationen über automatische Updates konnten wir nicht finden.

Personal Security

Diese Funktion schickt eine SOS-Nachricht an die eingetragene Handy-Nummer, sollte sich der Benutzer in Not befinden. Der Benutzer muss dafür den Einschaltknopf drei- bis fünfmal betätigen, um den Notfall-Modus zu aktivieren. Nach Aktivierung der Funktion schickt das Programm Details vom Standort mit SOS-Nachricht. Weiters wird eine Status-Meldung auf Facebook und Twitter gepostet.

Hilfe

Es werden sehr umfangreiche und hilfreiche Hilfedateien angeboten. Zusätzlich existieren noch FAQ, welche jedoch nicht besonders gut sortiert sind, wodurch man lange suchen muss bis man die Lösung zu einem Problem findet.

Deinstallation

Die Deinstallation wird über den Android Appmanager durchgeführt. Hierfür ist ein Passwort erforderlich. Also kann ein Dieb nicht einfach den Diebstahlschutz deaktivieren. Für mehr Komfort existiert zusätzlich ein Wizard, welcher bei der Deinstallation behilflich ist.

Lizenz

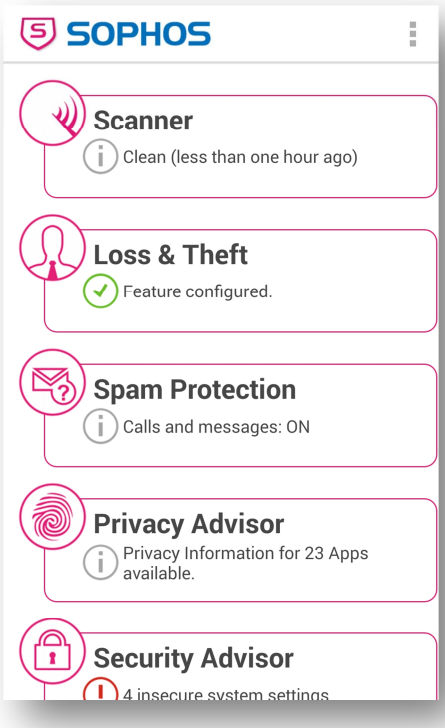
Quick Heal Total Security ist für 5,17€ im Google Play Store verfügbar.

Fazit

Quick Heal hat die Software im Vergleich zur Vorjahresversion optisch stark überarbeitet. Das Sicherheitsprodukt gehört hinsichtlich des Funktionsumfangs zu den Umfangreichsten. Neben den klassischen Diebstahlschutz-funktionen, für welche auch ein Webinterface zur Verfügung gestellt wird, bietet das Sicherheitsprodukt sinnvolle Funktionen wie Kindersicherung, Backupfunktion und weitere Komponenten.

Sophos Security and Antivirus

Sophos bietet mit *Security and Antivirus* ein Sicherheitsprodukt, das alle wichtigen Komponenten eines modernen Sicherheitsprodukts enthält und kostenlos zur Verfügung gestellt wird.



Installation

Sophos Security and Antivirus wurde aus dem Google Play Store bezogen und installiert. Nach der Installation muss lediglich den Lizenzvereinbarungen zugestimmt werden und der Benutzer landet auf der Startseite der Applikation. Nach der Installation wird ein initialer Malwarescan durchgeführt.

Starten des Programms

Beim Starten des Programms wird der Homebildschirm angezeigt. Dieser scheint sehr aufgeräumt und der Nutzer findet sich schnell zurecht.

Scanner

Der Scanner ermöglicht das Durchsuchen des Telefons nach schädlicher Software. In den Einstellungen kann der Benutzer festlegen ob Scans mithilfe der Cloud durchgeführt werden sollen. Es ist möglich, diesen Dienst für Roaming zu sperren, oder gar nur bei aktiver WiFi Verbindung zuzulassen. Es kann festgelegt werden ob der Scanner auch potentiell ungewollte Applikationen aufzeigen soll. Außerdem ist es möglich regelmäßige Scans in einem Zeitintervall von sechs Stunden bis zu drei Tagen durchzuführen. Sophos bietet außerdem einen Echtzeitschutz, der jede frisch installierte App sowie Änderungen von Dateien scannt.

Loss & Theft

Mit dieser Komponente ist es möglich, im Falle des Verlustes des Telefons, einen Alarm abzuspielen, das Gerät zu sperren, zu orten oder darauf befindliche Daten zu löschen. Dies geschieht durch Senden von SMS Nachrichten. Ein Webinterface wird nicht angeboten. Akzeptiert werden die Befehle jeweils nur von vertrauenswürdigen Nummern, die im Vorfeld definiert werden müssen. Zusätzlich benötigt der Sender ein Passwort um die Kommandos versenden zu können. Kommandos von anderen Nummern werden, selbst mit gültigem Passwort, ignoriert.
Gefallen hat uns, dass beim Starten der Diebstahlschutzkomponente eine schöne Übersicht geboten wird, die signalisiert welche der Komponenten aktiv sind, und welche noch einer weiteren Konfiguration bedürfen.

Lock

SMS Kommando: Lock <Passwort>

Dieses Kommando sperrt das Handy mit der eingestellten Android-Sperrmethode. Außerdem wird ein Icon mit einer Sperrnachricht eingeblendet. Der Sperrbildschirm ist allgemein sehr sicher und lässt sich nicht umgehen. Wird das Telefon erfolgreich gesperrt erhält der Sender eine Antwortnachricht.

Alarm

SMS Kommando: Alarm <Passwort>

Dieses Kommando sperrt den Bildschirm wie das *Lock* Kommando. Zusätzlich wird hier noch

ein Alarmsignal abgespielt. Dieses Verhalten könnte für einen Dieb abschreckend sein.

Locate

SMS Kommando: Locate <Passwort>

Nach dem Absetzen des Kommandos versucht das Telefon mittels GPS und WiFi seine Position zu bestimmen. Nach erfolgreicher Lokalisierung erhält der Sender eine Nachricht mit den Koordinaten und einem Link auf Google Maps. Der Benutzer erhält diese Nachricht zuerst mit einer ungefähren Position und nach einiger Zeit mit einer genaueren.

Locate at Low Battery

Ist diese Funktion aktiviert, so wird das Gerät jedes Mal geortet, wenn die Batterie schwach wird. In diesem Fall wird die Position an die vertrauenswürdige Nummer gesendet.

Unlock

SMS Kommando: Unlock <Passwort>

Dieser Befehl definiert ein neues zufällig gewähltes Passwort auf dem Gerät. Als Antwort erhält man eine SMS mit dem neuen Kennwort.

Wipe

SMS Kommando: Wipe <Passwort>

Beim Wipe hat sich Sophos besonders viel Mühe gegeben. Der Nutzer hat die Möglichkeit für verschiedene Datentypen verschiedene Sicherheitslevels zu definieren. Diese bestimmen dann, ob bei einem Wipe die Dateien nur gelöscht (Erste 8 kB der Datei werden überschrieben) oder komplett mit Junk überschrieben werden sollen. Letzteres hat zur Folge, dass der Wipe ein wenig länger dauert. Unser Test hat gezeigt, dass dies auch wie erwartet funktioniert. Die Dateien auf der SD-Karte wurden wie erwartet gelöscht. Die Daten konnten in unserem Test nicht wiederhergestellt werden.

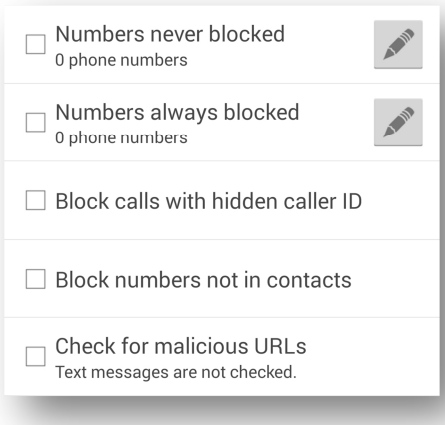
SIM Change

Wird die SIM-Karte des Geräts getauscht, versendet das Handy eine Nachricht mit IMEI und IMSI an alle eingetragenen vertrauenswürdigen Nummern. Dabei wird das Gerät mit dem Android Lock Screen gesperrt.

Spam Protection

Die Spam Protection schützt den Nutzer vor unerwünschten Anrufen und SMS. Obwohl die Schutzfunktionen jeweils global ein- und ausgeschalten werden können, ist dies für einzelne Nummern nicht möglich, so ist es z.B. nicht möglich die nur die SMS Nachrichten einer Nummer zu blockieren. Über ein intuitives Menü können Nummern zu einer Liste hinzugefügt werden, deren Einträge nie blockiert werden sollen. Das Gleiche ist für eine weitere Liste möglich, deren Einträge immer blockiert werden. Sollte eine Nummer auf beiden aufscheinen, so greift die Whitelist. Optional kann der Nutzer Anrufe und SMS blockieren lassen, die die Nummer unterdrücken, oder nicht in der Kontaktliste vorhanden sind.

Ist der SMS Blocker aktiv, kann Sophos vor schadhaften URLs, wie zum Beispiel Links zu Phishingseiten, in Textnachrichten schützen.


Numbers never blocked
0 phone numbers
Numbers always blocked
0 phone numbers
Block calls with hidden caller ID
Block numbers not in contacts
Check for malicious URLs
Text messages are not checked.

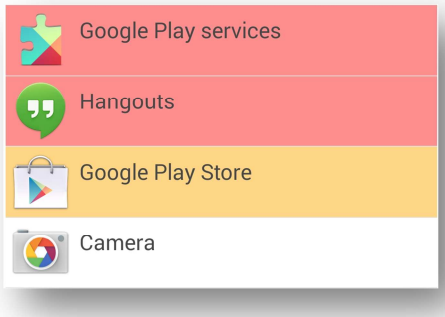
Die gesamte Blockierfunktion von SMS hat in unserem Test auf dem Nexus 5 Testgerät nicht funktioniert. Auf dies wurde von Sophos auch entsprechend hingewiesen. Sophos verspricht jedoch, dass dieser Zustand in folgenden Releases behoben werden soll. Auf dem alternativen Testgerät mit Android 4.1.2 hat die Funktion jedoch wie erwartet funktioniert.

Die Blockierfunktion von Telefonanrufen hat wie erwartet geklappt. Hier ist nur zu

bemerken, dass der Anruf für einen Bruchteil einer Sekunde aufscheint.
In einer Quarantäne können in der Vergangenheit geblockte SMS und Anrufe eingesehen werden und dort angezeigt, wiederhergestellt oder gelöscht werden.

Privacy Advisor

Der Privacy Advisor listet jene installierten Apps, die für den Nutzer eine Bedrohung bezüglich der Verletzung der Privatsphäre darstellen können. Sophos kategorisiert die Apps nach Bedrohungsstufe (hoch, mittel, niedrig) und färbt die Apps in der Liste mit rot, gelb und weiß ein.



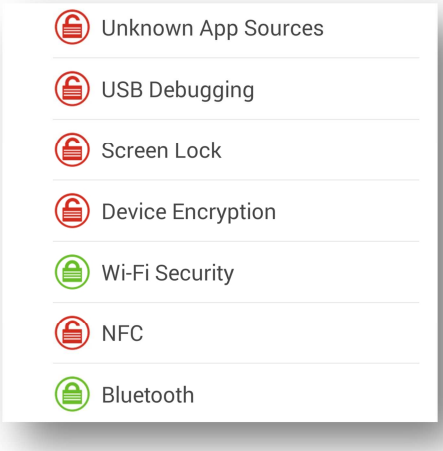
Der Nutzer hat die Möglichkeit nach folgenden Bedrohungsarten zu filtern: Apps die Kosten verursachen, auf persönliche Informationen oder auf das Internet zugreifen können. Durch Antippen einer Applikation werden die Berechtigungen sehr detailliert beschrieben.

Security Advisor

Der Security Advisor macht den Nutzer auf Einstellungen auf dem Telefon aufmerksam, die die Sicherheit beeinträchtigen könnten. Sophos überprüft sieben Einstellungen z.B. ob eine Bildschirmsperre oder eine Geräteverschlüsselung aktiviert ist. Durch Klicken auf einen der Einträge wird der Nutzer zu einer Erklärung und einem Button, der direkt zur entsprechenden Einstellung in den Android Settings führt, geleitet.

App Protection

Diese Komponente ermöglicht das Schützen von installierten Apps mit einem mindestens vierstelligen Passwort. Nachdem dieses eingestellt wurde, erscheint eine Warnung, dass sich die App Protection mithilfe von Taskmanagern umgehen lässt. Hierfür bietet Sophos Abhilfe durch ein weiteres App, Sophos Security & Antivirus Guard, das sicherstellt, dass die Sicherheitssuite nie beendet wird.
Der einstellbare Parameter *Grace Period* definiert jene Zeit, für die das App nach dem Entsperren ohne weitere Passworteingabe zugänglich bleibt, bevor es wieder gesperrt wird. Als Voreinstellung hat Sophos fünf Minuten gewählt.

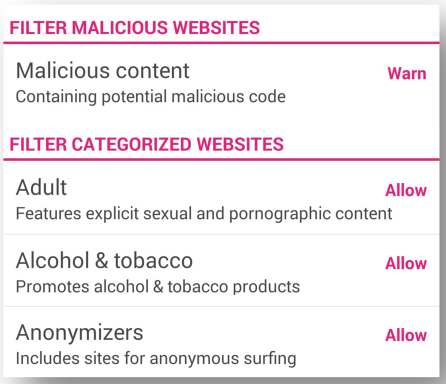


Als Selbstschutz hat Sophos sich selbst, sowie die Android Einstellungen mit einem Passwort versehen. Dieser kann nicht deaktiviert werden. Aus einer Liste können weitere installierte Apps gewählt werden, welche ebenfalls mit demselben Kennwort versehen werden sollen.
In unseren Tests hat diese Funktion sehr verlässlich funktioniert und konnte nicht umgangen werden.

Web Filtering

Diese Komponente schützt den Nutzer während des Surfens im Internet vor schadhaften Webseiten. Zusätzlich kann nach Inhalten gefiltert werden, wie etwa Alkohol, Drogen, Waffen und weitere. All diese Kategorien sind standardmäßig auf „allow“ gesetzt. Diese Komponente lässt sich somit auch als Kindersicherung einsetzen. In

unseren Tests hat diese Komponente sehr gut und verlässlich funktioniert.
Die Menüführung ist jedoch nicht sehr verständlich gestaltet. Zum einen existieren Buttons mit der Aufschrift „Allow“ (deutsch „erlauben“) welche den Status „signalisieren, dass die jeweilige Kategorie erlaubt sein soll. Dadurch, dass es sich um klickbare Buttons handelt, könnte man dies auch missverstehen und davon ausgehen, dass ein Tippen auf „Allow“ die jeweilige Kategorie erlaubt.
Eigenartig ist auch, dass sich zwischen diesen Kategorien auch „Phishing & Fraud“, sowie „Spyware“ findet. Auch diese sind standardmäßig auf „allow“ gesetzt. Wir finden, dass diese Kategorien in die Kategorie „Malicious Websites“ verschoben und standardmäßig zumindest auf „Warn“ oder gar „Block“ gesetzt sein sollten. Sophos hat uns darüber informiert, dass es sich bei den genannten Kategorien um Webseiten handelt, welche Spywaretools für kriminelle Zwecke zur Verfügung stellen.



Nachdem wir verstanden haben, wie der Filter tatsächlich arbeitet, hat die Komponente gut und verlässlich gearbeitet.

Updates

Wir konnten keine Informationen bezüglich Updates finden. Sophos gibt lediglich an, dass der Nutzer bei Verwendung von Cloudscans stets die aktuellsten Virendefinitionen geboten bekommt.

Hilfe

Sophos bietet dem Nutzer zu jeder Komponente eine ausführliche Hilfe in Form von Infoboxen an. Diese halten wir für die ausreichend.

Deinstallation

Es wird kein Assistent zum Deinstallieren angeboten. Sophos hat uns jedoch darüber informiert, dass dieser für die kommende Version geplant sei. Beim Security Advisor steht ein Hinweis, dass für eine Deinstallation des Programms der Geräteadministrator deaktiviert werden muss. Danach kann das Produkt über den Android App Manager deinstalliert werden.
Weder für die Deaktivierung des Geräteadministrators noch für die eigentliche Deinstallation musste ein Passwort eingegeben werden. Ein Dieb könnte somit den Diebstahlschutz schnell außer Kraft setzen. Somit empfiehlt es sich die ebenfalls integrierte App-Protection zu aktivieren, wodurch eine Passworteingabe für die Deinstallation erforderlich wird. Sophos weist auf diesen Zustand jedoch nicht explizit hin. Sophos hat auf unsere Anfrage hin angemerkt, dass dies in der kommenden Version implementiert wird.

Lizenz

Sophos Security and Antivirus ist kostenlos und uneingeschränkt nutzbar.

Fazit

Sophos hat im Test überzeugt. Das kostenlose Programm bietet viele sinnvolle Funktionen die aktiv zur Sicherheit des Nutzers beitragen. Gefallen hat uns der Security Advisor, welcher auf mögliche kritische Einstellungen hinweist, sowie eine gut gestaltete Spam Protection Komponente.

Tencent Mobile Manager

Tencent Mobile Manager ist kostenlos verfügbar und bringt einen großen Funktionsumfang und viele optional installierbare Add-Ons mit sich. Tencent hat die Applikation erneut mit neuen Funktionen ausgestattet.

Installation und Starten des Programms

Die Installationsdatei wurde von der Webseite des Herstellers bezogen und installiert. Im ersten Schritt muss die Lizenzvereinbarung akzeptiert werden (standardmäßig aktiv). Außerdem fordert Tencent den Nutzer dazu auf, das Tencent Nachrichtenmodul als Standardapplikation für das Senden und Empfangen von SMS Nachrichten einzutragen.

Nach dem erfolgten ersten Start des Programms wird ein „Mobile Phone Health Check" automatisch gestartet. Die resultierenden Punkte werden in der Mitte des „Check-Up & Speed Up" Tabs dargestellt. Der Nutzer kann das Gerät durch Tippen auf das Kreissymbol optimieren. Die Funktion beendet laufende Prozesse, gibt belegten RAM frei und löscht nicht mehr benötigte Dateien.

Nach Durchführung dieser Aktion wird das Gerät mit einer Gesundheit von 95 Punkten bewertet. Weitere fünf Punkte erhalten wir durch die Aktivierung des „Payment Protection" Features.

Health optimisation tab

In dieser Ansicht der Applikation bietet Tencent einen „Mobile Speed-up", einen „Data Traffic Manager", sowie Links zu Downloadseiten von Energie- und Speichermanagern.

Data Volume Manager

Diese Komponente zeigt den täglichen und monatlichen Verbrauch des Datenvolumens. Das monatliche Volumen bezieht sich auf den Mobilfunkvertrag des Nutzers, dessen Rahmenbedingungen in den Einstellungen gesetzt werden können. Mit unserer Prepaid SIM Karte von Unicorn hat die Überprüfung wie erwartet funktioniert.

Space cleaning

Diese Funktion räumt das Gerät auf und löscht im Zuge dessen den WeChat Speicher, App Caches, nicht mehr benötigte Dateien, Betriebssystem Cache und Überbleibsel von deinstallierten Applikationen. Nach

Durchführung der Bereinigung werden wir dazu aufgefordert den „WeChat“ Speicher manuell zu bereinigen.

Energy Manager

Hierbei handelt es sich um eine Applikation, welche separat installiert werden muss.

Storage Manager

Diese Komponente sucht nach kaum verwendeten Apps, sowie Videodateien und Fotos. Fotos und Videos können auf die externe SD Karte verschoben werden.

Security Protection Tab

In dieser Ansicht werden all jene Funktionen gelistet, die die Sicherheit betreffen. Folgende sind verfügbar:

Nuisance Calls and Text Spam

Tencent hat diese Funktion integriert um den Nutzer vor unerwünschten Anrufen und Spam SMS zu schützen. Zudem wird eine Back- und Whitelisting Funktion geboten. Außerdem ist es möglich Nummern, welche Spam verbreiten an Tencent zu melden.

In unserem Test hat Tencent zurecht mehrere Telefonnummern geblockt, welche für unerwünschte Telefonanrufe verantwortlich waren.

Payment protection

Diese Funktion bietet eine sichere Umgebung für Applikationen wie Alipay Wallet und WeChat. Diese Applikationen können direkt aus dieser Ansicht aus gestartet werden. Bevor jene Applikationen gestartet werden, wird darauf hingewiesen, dass zuvor der Phishing Schutz, und QR Code Schutz aktiviert wird und das WLAN Netzwerk auf dessen Sicherheit überprüft wird.

Privacy Protection

Unter dieser Registerkarte werden Funktionen zusammengefasst, welche den Schutz der Privatsphäre des Nutzers betreffen. Folgende Komponenten werden angeboten:

Privacy Space

Für die Nutzung dieser Komponente muss erst ein Passwort in Form einer Geste definiert werden. Dieses wird benötigt um Textnachrichten von bestimmten Telefonnummern zu verstecken, ebenso wie Fotos, Videos und andere Dateien.

Wenn der Nutzer zum Beispiel Fotos zu den versteckten Dateien hinzufügt, so werden diese in einem eigenen Album innerhalb des Privacy Guard Tools angezeigt, jedoch nicht mehr im normalen Album. Für die Anzeige ist anschließend ein Kennwort erforderlich.

App Permissions

Hier werden installierte Applikationen gelistet und entsprechend ihren Berechtigungen eingeteilt. Die Funktion kann behilflich sein um mögliche Verletzungen der Privatsphäre durch installierte Apps auszuspüren.

AV Scan

Laut Beschreibung in der Applikation scannt diese Komponente das System nach Lecks, schadhaften Applikationen und Gefahren während des Bezahlens.

In den Einstellungen kann konfiguriert werden, ob ein „Smart Scan“, „Quick Scan“ oder ein „Full Scan“ durchgeführt werden soll. Zudem kann eine weitere Komponente, ein Tool zum Entfernen von Trojanern, installiert werden.

Anti Theft

Diese Komponente ist nicht standardmäßig aktiviert. Für die Verwendung muss erst ein Kennwort definiert, sowie die Telefonnummer einer Vertrauensperson angegeben werden, welche informiert wird wenn die SIM Karte getauscht wird.
Die gesamte Komponente wird mit englischsprachigen Textnachrichten gesteuert.

Delete

SMS Command: „#QQDeleteALL#password

Dieser Befehl löscht alle persönlichen Daten vom Gerät des Nutzers. Dabei wird es nicht auf Werkseinstellungen zurückgesetzt. Dies hat den Vorteil, dass der Diebstahlschutz weiterhin aktiv bleibt. In unserem Test wurden SMS, Kontakte, und Fotos gelöscht. Vergessen wurde jedoch auf den Google Account. Da Google Dienste in China nicht sehr gängig sind, sehen wir dies als kein sehr großes Risiko an. Allerdings verblieben auch Nachrichten von WeChat auf dem Gerät, auch in der dazugehörigen App waren wir immer noch eingeloggt.

Lock

SMS Command: „#QQLock#password

Diese Funktion sperrt das Gerät und verhindert somit den Zugriff Unbefugter auf das Gerät. Um das Gerät zu entsperren muss das zuvor definierte Kennwort eingegeben werden, wofür im Übrigen sein simples „1“ akzeptiert wurde. Solch kurze Kennwörter sind nicht sicher, worauf Tencent aufmerksam machen sollte.
Nach Abschluss unseres Reviews veröffentlichte Tencent eine neue Version der Software, welche die Verwendung der Diebstahlschutzes nur noch unter Angabe eines QQ Accounts erlaubt. Die Verwendung von Passwörtern wird nicht mehr angeboten.

Locate

SMS Command: „#QQLocate#password

Diese Funktion ortet ein gestohlenes oder verlorengegangenes Gerät. Der Absender des Kommandos erhält nach dem Absetzten des Befehls eine Antwort mit einer Beschreibung zum Wiederfinden, sowie einem Link zu einem Kartendienst.

Recover Password

SMS Command:
„#QQPIN#registered emergency number“

Diese Funktion ermöglicht es dem Nutzer sein Kennwort zurückzusetzen. Diese Operation kann nur von der Nummer der Vertrauensperson durchgeführt werden.

Program Manager Tab

Diese Ansicht von Tencent ermöglicht es dem Nutzer Apps und Spiele herunterzuladen, Apps zu aktualisieren, und zu deinstallieren. Zudem werden ein Package- und ein Berechtigungsmanager angeboten.

Über diese Ansicht ist es zudem möglich den eigenen Appstore von Tencent zu durchsuchen. Die restlichen Funktionen ermöglichen es dem Nutzer Updates zu verwalten und Apps zu deinstallieren. Ein eine Reinstallationsfunktion macht es zudem möglich Apps aus APK Dateien, welche auf dem Gerät verfügbar sind, zu installieren. Die APK Dateien werden sortiert nach Quelle, also zum Beispiel dem Tencent Download Channel oder anderen Quellen. Des Weiteren werden

Additional Tools

Durch Antippen des Symbols mit vier Quadraten in der oberen Ecke der Oberfläche erreicht der Nutzer erweiterte Tools, wie zum Beispiel ein „Mobile-Fee" Scanner. Zu den bereits installierten, können noch weitere verfügbare Tools installiert werden, wie etwa ein „Router Manager", ein „Battery Doctor" oder einem Assistenten zum Migrieren von Dateien auf ein neues Smartphone.
Zusätzlich werden auch Sicherheitsrelevante Funktionen geboten, wie zum Beispiel ein Ad-Detektor, welcher eingehende SMS Nachrichten verdächtigen Inhalten prüft.
In unserem Test wurden 10 eingehende Nachrichten der Taxi App „Didi" geblockt. SMS der Taxi App „Kuaidi" wurden hingegen einfach durchgelassen. In einem Update von Kingsoft, welches nach der Erstellung des Reviews veröffentlicht wurde, wurde diese Funktion entfernt.

Unserer Meinung nach sticht der Schutz der WeChat App zu wenig ins Auge und kann leicht übersehen werden. Dieser Schutz schützt vor unerlaubter Verwendung der WeChat App, deren Nachrichten auch durch Absetzen des Wipe Kommandos nicht gelöscht werden.

Tencent Rocket

Nach der Installation der App war auf dem Desktop unseres Testgeräts ein kleines Icon eingeblendet, welches veranschaulicht wie viel Speicher gerade verwendet wird. Durch Ziehen der Grafik an das untere Ende des Bildschirms führt Tencent eine Bereinigung durch, beendet laufende Prozesse und gibt Speicher frei.

Deinstallation

Vor der Deinstallation wird der Nutzer über den Grund der Deinstallation gefragt. Ein Assistent für die Deinstallation ist jedoch nicht verfügbar. Zudem ist kein Passwort erforderlich. Dies kann problematisch sein, da ein Dieb den Diebstahlschutz somit einfach deinstallieren könnte.

Lizenz

Tencent Mobile Manager ist kostenlos verfügbar.

Hilfe

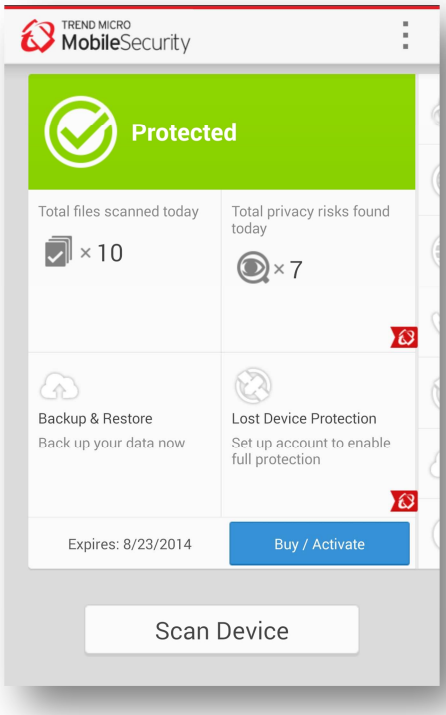
Alle Funktionen werden innerhalb der Applikation erläutert und Hilfe in Form von kurzen Texten geboten.

Fazit

Tencent bietet mit Mobile Manager ein Sicherheitsapp mit einer Vielzahl von Funktionen. Das Blockieren von unerwünschten Telefonanrufen hat in unseren Tests gut funktioniert. Wir möchten die Empfehlung aussprechen bei einem Wipe die Kennwörter von Google und WeChat zu löschen, sowie die Deinstallation mit einem Kennwort zu schützen.

Trend Micro Mobile Security

Mobile Security von Trend Micro bietet neben den wichtigsten Schutzfunktionen wie dem Diebstahlschutz und Malwarescanner zusätzlich sinnvolle Erweiterungen wie sicheres Surfen und Kindersicherung.



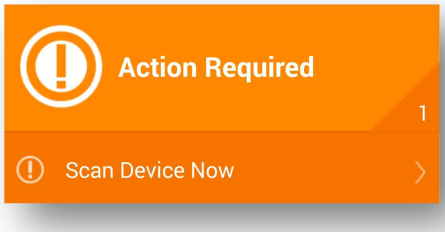
Installation

Wir haben Trend Micro aus dem Google Play Store bezogen und installiert. Nach dem Akzeptieren der Lizenzvereinbarungen wird bereits der Startbildschirm angezeigt.

Starten des Programms

Beim ersten Start bekommt der Nutzer eine kurze Einführung in das Produkt und die Bedienung, wie z.B. der Wischgeste nach rechts, um zu den erweiterten Funktionen zu gelangen. Über eine Infobox wird signalisiert, dass sich der Nutzer mit seinem Trend Micro Account anmelden, oder einen solchen registrieren möge. Außerdem wird durch eine hervorstechende, orange Box signalisiert, dass der Nutzer einen Malwarescan durführen möge.

Auf dem Startbildschirm befinden sich Schnellwahlbuttons zu Ergebnissen des Malware Scanners, des Data Theft Scanners, sowie der Backup- und Anti-Theft Komponente. Am unteren Bildschirmrand befindet sich ein Button, welcher das Schnelle Scannen des Geräts ermöglicht.

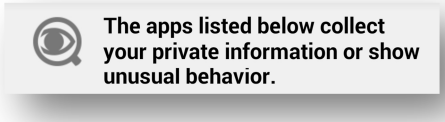


Virus Scanner

Durch Klick auf den Button für den Virus Scanner wird der Nutzer entsprechend weitergeleitet. Auch dort findet sich ein Button zum sofortigen Scannen des Geräts, sowie einer Vielzahl von Einstellmöglichkeiten, unter anderem ob die die SD Karte gescannt, oder der Echtzeitscanner aktiviert werden soll. Optional kann nach jedem Update ein Scan durchgeführt werden. In einer Historie werden Aktionen von Scans und Updates aufgelistet.

Privacy Scanner

Der Privacy Scanner überprüft die auf dem Gerät installierten Apps auf mögliche Risiken bezüglich der Spionage von privaten Daten oder aggressiven Werbungen. Trend Micro bietet für diese Komponente auch einen Echtzeitscanner, der bei der Installation von neuen Programmen sofort eine derartige Überprüfung vornimmt.

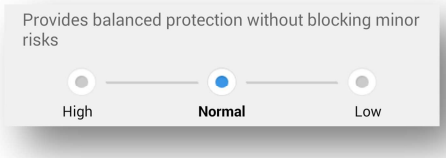


Mögliche Bedrohungen werden in Gefahrenkategorien eingeteilt. Dies erschien uns in unseren Tests auch schlüssig. So sind fragwürdige Applikationen als „Medium Risk“ eingeteilt worden, bekannte Apps wir Opera Browser als „Low Risk“. Durch Antippen eines Eintrags werden Details zu den jeweiligen Berechtigungen, sowie eine kurze Erklärung angezeigt. Anschließend kann die Applikation

entweder deinstalliert oder einer Liste von vertrauenswürdigen Apps hinzugefügt werden.

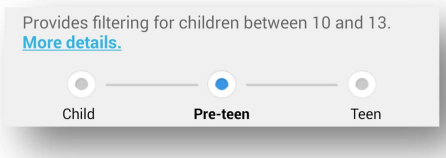
Safe Surfing and Parental Control

Unter dieser Komponente fasst Trend Micro Schutzfunktionen bezüglich des Surfens im Internet, sowie Kindersicherung, zusammen.



Das Safe Surfing schützt den Nutzer beim Browsen im Internet. Dabei kann als Sicherheitsstufe hoch, mittel oder niedrig eingestellt werden. Während bei „hoch" Webseiten mit jedem geringsten Risiko geblockt werden, ist Trend Micro mit der Einstellung „niedrig" ein wenig nachsichtiger und ignoriert weniger gefährliche Bedrohungen.

Für Parental Control muss erst das Kennwort des Trend Micro Accounts eingegeben werden. Danach kann ein Schutz speziell für den internetsurfenden Nachwuchs eingestellt werden. Hierbei hat der Nutzer die Möglichkeit den Schutz speziell auf das Alter abzustimmen. Zusätzlich zur Voreinstellung können Webseiten auf eine Black- oder Whitelist gesetzt werden.



Mit der Uninstall-Protection kann verhindert werden, dass das Kind oder der Jugendliche das App einfach deinstalliert. Diese Funktion würden wir nicht nur dem Jugendschutz zuordnen, sondern z.B. auch dem Diebstahlschutz. Deshalb würden wir einen globalen Deinstallationsschutz für sinnvoller befinden.

Im Gegensatz zur Vorjahresversion hat der Deinstallationsschutz im diesjährigen Test sehr gut funktioniert. Vor der Deinstallation war eine Passworteingabe notwendig, die wir nicht umgehen konnten.

In einer Historie können geblockte Webseiten angezeigt werden. Dies trifft sowohl für gefährliche Homepages zu, als auch für solche die aufgrund des Jugendschutzes blockiert wurden.

Call Blocking

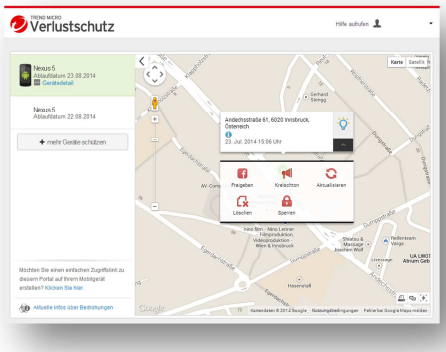
Trend Micro bietet das Blockieren von unerwünschten Anrufen. Hierfür kann entweder Blacklisting oder Whitelisting gewählt werden. Während dem Whitelisting kann noch die Option aktiviert werden, dass Anrufer mit unterdrückter Nummer akzeptiert werden.

Zusätzlich lässt sich die Aktion einstellen, welche bei einer erfolgreichen Sperrung ausgeführt werden soll. Hierfür stehen dem Nutzer die Möglichkeiten „Abweisen", „Gerät stumm stellen" und „Abweisen + SMS Antwort senden" zur Verfügung. Für die SMS Antwort kann entweder einer der drei vordefinierten Texte, oder ein manuell eingegebener gewählt werden.

Die Blockierung von SMS wurde auf unserem Testgerät nicht angeboten. Auf dem alternativen Gerät mit Android 4.1.2 war die Option jedoch eingeblendet und hat funktioniert. Diese Vorgehensweise finden wir eigentlich sehr gut, da dem Nutzer nur jene Funktionen angeboten werden, die auch funktionieren, anstatt mit Infoboxen auf Fehlfunktionen hinzuweisen.

Lost Device Protection

Unter Lost Device Protection versteht Trend Micro den Diebstahlschutz. Es werden die klassischen Schutzfunktionen wie Lokalisieren, Sperren und Löschen angeboten. Gesteuert werden die Kommandos über ein Webinterface. SMS Kommandos existieren nicht.



Zum Ändern jeglicher Einstellungen betreffend der Lost Device Protection ist ein Passwort erforderlich, damit ein Dieb nicht einfach die Diebstahlsicherung deaktivieren kann.

Locate

Die Locate Funktion lokalisiert ein gestohlenes oder abhandengekommenes Gerät und zeigt die Position in einer Google Maps Karte an. Die Aktion wird automatisch ausgeführt, wenn das Webinterface geöffnet wird. Die Position kann auf Facebook geteilt werden.

SIM Card Lock

Der SIM Card Lock sperrt das Gerät, wenn die SIM Karte entweder entnommen oder eine andere eingelegt wird.

Der SIM Lock hat in unserem Test sehr lange gedauert. Ein Dieb hat somit die Möglichkeit nach einem Neustart des Geräts es für rund 45 Sekunden uneingeschränkt zu verwenden.

Lock

Mit dieser Funktion wird das Gerät gesperrt und somit der Zugriff für Dritte unmöglich gemacht. Es kann nur mit einem gültigen Passwort wieder entsperrt werden.

Es besteht die Möglichkeit Notrufe zu tätigen und es ist dem Nutzer möglich ein neues Passwort via E-Mail zu versenden.

Die Lockfunktion wurde im Vergleich zur Vorjahresversion stark verbessert. Wir konnten weder die Notification-Leiste öffnen, noch den Sperrbildschirm auf irgendeine Weise umgehen.

Sirene

Dieser Befehl lässt einen sehr lauten Alarm ertönen. Dabei wird das Gerät nicht gesperrt, es dient also nur dem Wiederfinden innerhalb der eigenen vier Wände.

Wipe

Beim Wipe bietet Trend Micro zwei Varianten an: Den Partial Remote Wipe, der persönliche Daten vom Gerät löscht, und einen Full Remote Wipe, der zusätzlich das Gerät auf Werkseinstellungen zurücksetzt.

Der Wipe hat im Großen und Ganzen gut funktioniert, jedoch konnten ein Großteil der Daten von der externen SD Karte mit gängigen Gratistools wiederhergestellt werden. Trend Micro hat uns darüber informiert, dass das vollständige Löschen inklusive Überschreiben des Speichers sehr viel Batterie verbrauchen würde und die Gefahr bestünde, dass der Akku vor Abschluss der Operation ausgehen könnte.

Backup& Restore

Diese Funktion ist als externe App verfügbar und ermöglicht die Sicherung von Kontakten, Kalendereinträgen, Anruf History, Text History, Fotos, Musik und Videos. Hierfür bietet Trend Micro 50MB Speicher.

Das Backup kann auch automatisch gestartet werden. Hierfür können die Wochentage eingestellt werden. Außerdem besteht die Möglichkeit das Automatische Backup für Roaming und mobile Datenverbindung zu deaktivieren. Auch die Rücksicherung gestaltet sich komfortabel. Trend Micro prüft alle Änderungen auf dem Server und schlägt anschließend vor, welche Einträge zurückgesichert werden könnten.

Facebook

Diese Komponente ist als zusätzliche Applikation verfügbar und prüft das Facebookprofil des Nutzers auf datenschutzrechtlich bedenkliche Einstellungen. Dazu muss der Nutzer den Usernamen und das Passwort seines Facebookaccounts angeben. Anschließend werden alle „Privacy Concerns“ aufgelistet,

zum Beispiel ob die Personalisierung auf Partnerseiten erlaubt sein soll, oder ob der Nutzer vor der Markierung in Beiträgen anderer Nutzer zuvor eine Bestätigung erteilen können soll. Sollte der Nutzer eine Einstellung ändern wollen, so kann er dies direkt aus dem Menü tun. Trend Micro ändert selbstständig die entsprechenden Einstellungen in Facebook.

Updates

Updates können manuell oder automatisiert durchgeführt werden. Für letzteres kann der User entscheiden ob diese täglich, wöchentlich oder monatlich durchgeführt werden sollen. Außerdem kann bestimmt werden, ob Updates nur bei aktiver WiFi Verbindung erlaubt sind.

Hilfe

Trend Micro bietet eine sehr umfangreiche Hilfe an. Diese ist sowohl detailreich als auch übersichtlich.

Deinstallation

Die Deinstallation kann über den androidinternen Anwendungsmanager deinstalliert werden. Hierfür ist kein Passwort notwendig, es sei denn der Nutzer hat die Kindersicherung aktiviert. In diesem Fall ist eine Passworteingabe erforderlich, welche wir nicht umgehen konnten. Hier stellen wir uns die Frage, warum der Deinstallationsschutz nicht global gesetzt werden kann, sodass es zum Beispiel auch Dieben nicht möglich ist den Diebstahlschutz zu deinstallieren.

Lizenz

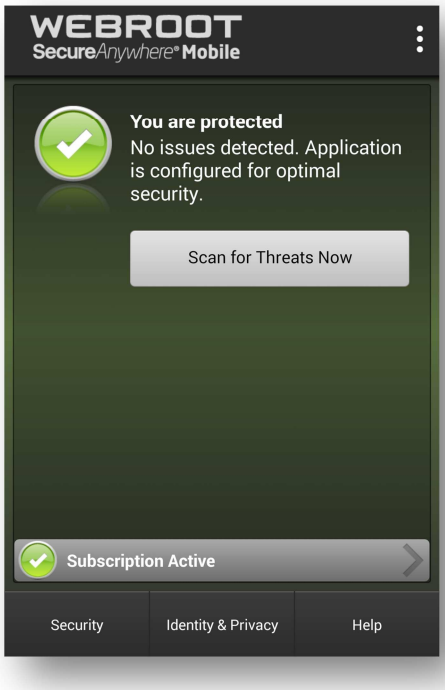
Trend Micro MobileSecurity kann kostenlos verwendet werden. Für die Premiumfunktionen Sicheres Surfen, Kindersicherung, Orten, Sperren, Löschen, SIM Lock und dem Schutz vor Deinstallation muss eine Lizenz erworben werden, die für 1 Jahr gültig ist und für 19,95€ erhältlich ist. Die Premiumfunktionen können für 30 Tage kostenlos getestet werden.

Fazit

Trend Micro bietet dem Nutzer sinnvolle Schutzmechanismen für Android Smartphones. Gefallen hat uns vor allem die Kindersicherung, die sehr ausgereift wirkt. Der hierfür verfügbare Deinstallationsschutz sollte jedoch auf die gesamte Applikation ausgeweitet werden. Erfreulich ist, dass die Mängel, die wir im letztjährigen Mobile Review kritisiert haben, durchwegs behandelt und behoben wurden.

Webroot SecureAnywhere Mobile Complete

Webroot bietet mit SecureAnywhere Mobile Complete ein ausgewogenes Sicherheitsprodukt an, welches in einer abgespeckten Variante frei verfügbar ist. Nutzer mit höheren Ansprüchen können die Premiumversion erwerben, welche einen noch größeren Funktionsumfang bietet.



Installation

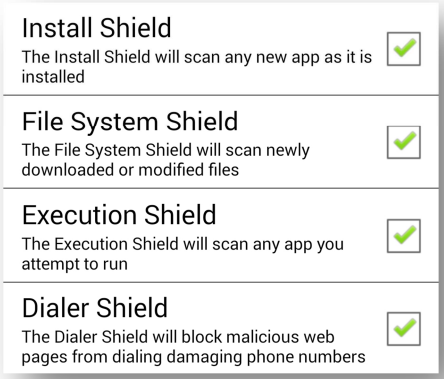
Webroot wurde aus dem Google Play Store geladen und installiert. Nach dem Akzeptieren der Lizenzvereinbarungen muss sich der Nutzer entweder mit seinem Webroot Account anmelden oder einen solchen registrieren. Hierfür muss ein Passwort vergeben werden, das aus mindestens sechs Zeichen besteht. Im Anschluss wir das Produkt als Geräteadministrator registriert.

Starten des Programms

Beim ersten Starten des Programms erscheint eine gelbe Warnmeldung, die signalisiert, dass wir keinen Android Lock Screen aktiviert, und die Installation von Apps aus unbekannten Quellen aktiviert haben. Nach der Behebung dieses Problems wird die Warnmeldung grün, die deutlich macht, dass das Gerät nun geschützt ist. Gleichzeitig wird automatisch ein Virus Scan durchgeführt.

Anti-Virus

Die Anti-Virus Komponente von Webroot schützt den Nutzer vor bösartiger Software. Über die Einstellung "Shields" können vier verschiedene Echtzeitschutzfunktionen aktiviert werden. Diese Funktionen sind Echtzeitschutz während der Installation, eine Überwachung des Dateisystems, ein Schutz beim Ausführen von Apps, sowie ein Schutz vor Dialern.

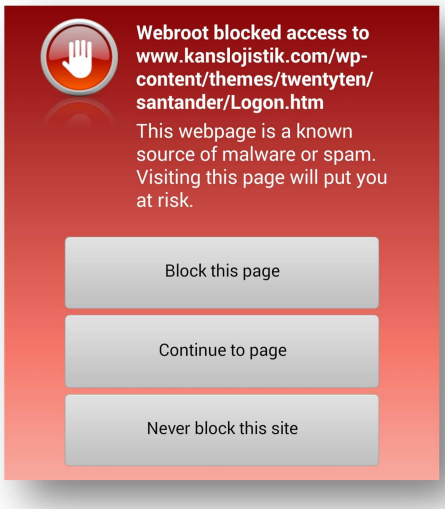

Install Shield
The Install Shield will scan any new app as it is installed
File System Shield
The File System Shield will scan newly downloaded or modified files
Execution Shield
The Execution Shield will scan any app you attempt to run
Dialer Shield
The Dialer Shield will block malicious web pages from dialing damaging phone numbers

Zusätzlich wird ein automatischer Malwarescan angeboten, dessen Frequenz zwischen stündlich, täglich und wöchentlich wählbar ist. Das Gleiche gilt auch für automatische Updates. Alternativ können diese auch manuell angestoßen werden.

Secure Web Browsing

Das Secure Web Browsing schützt den Nutzer beim Surfen im Internet. Bei der Blockierung einer Webseite kann der Nutzer diese als sicher bewerten, wenn er der Meinung ist, dass sie zu Unrecht gesperrt wurde. Webroot wird diese dann in Zukunft nicht mehr blockieren.

In unserem Kurztest hat diese Komponente mit Google Chrome ohne Probleme funktioniert.


Webroot blocked access to www.kanslojistik.com/wp-content/themes/twentyten/santander/Logon.htm
This webpage is a known source of malware or spam. Visiting this page will put you at risk.
Block this page
Continue to page
Never block this site

Lost Device Protection

Der Diebstahlschutz wird über SMS oder ein Webinterface (https://my.webrootanywhere.com) gesteuert. Letztgenanntes ist schön und intuitiv gestaltet und lässt die Verwaltung mehrerer Geräte zu. Dort lassen sich für jedes Gerät auch Informationen zum Schutzstatus, sowie Logs von diversen Events wie Malwarefunden anzeigen.

Scream

SMS Kommando: "scream <Password>"

Diese Funktion sperrt das Gerät und lässt währenddessen ein schrilles Geräusch ertönen. Gleichzeitig wird das Gerät gesperrt. Der Alarm kann durch einfaches Tippen deaktiviert werden.

Lock

SMS Kommando: "lock <Password>"

Diese Funktion sperrt das Gerät um einem Dritten den Zugriff auf das Smartphone des Nutzers zu verwehren. Obwohl im Hintergrund der Android Lock Screen verwendet wird, welcher sich nicht umgehen lässt, wird ein eigener Sperrbildschirm angezeigt. Dort erscheint auch eine Nachricht für z.B. einen ehrlichen Finder, die sich über das Webinterface ändern lässt.

Wipe

SMS Kommando: "Wipe <Password>"

Nach Absetzen des Kommandos wird das Gerät erst gesperrt und dann persönliche Daten gelöscht. Hierbei wird das Gerät auf Werkseinstellungen zurückgesetzt. Auf unserem alternativen Testgerät mit Android 4.1.2 wurden die Dateien auf der externen SD Karte nicht gelöscht.

Locate

SMS Kommando: "Locate <Password>"

Diese Funktion dient dem Wiederfinden eines verlorenen oder gestohlenen Geräts. Während der Lokalisierung wird das Gerät gesperrt. Setzt der Nutzer das Kommando über das Webinterface ab, so wird nach erfolgreicher Lokalisierung die Position in einer Google Maps Karte dargestellt. Während der Positionsfindung lassen sich keine anderen Kommandos mehr absetzten. Dies kann vor allem dann problematisch sein, wenn das Orten länger dauert.

Wird der Befehl per SMS abgeschickt erhält der Sender eine Antwort mit einem Link auf Google Maps mit den entsprechenden Koordinaten.

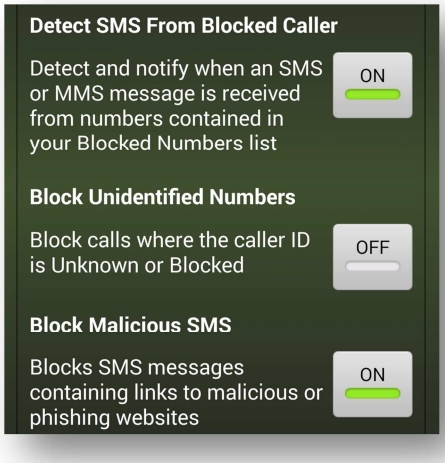
SIM Lock

Auch diese Funktion ist nur in der Premium Version verfügbar. Nach dem Entfernen der vertrauenswürdigen SIM Karte und anschließendem Neustart wird das Gerät gesperrt. Ein Dieb hat somit nicht die Möglichkeit das Gerät mit seiner eigenen SIM Karte zu nutzen.

Call & SMS Blocking

Diese Komponente schützt vor unerwünschten Anrufen und SMS. Webroot verfolgt hierbei den Ansatz des Blacklistings. Der Nutzer kann bekannte Störenfriede auf diese Liste setzen, welche anschließend keine Möglichkeit mehr haben mit ihm Kontakt aufzunehmen. Nummern können entweder manuell eingegeben, oder aus den Kontakten, dem Anruflog oder dem SMS-Log importiert werden. Zusätzlich können mit dieser Komponente Anrufer, die ihre Nummer unterdrücken, blockiert werden. Weiters bietet

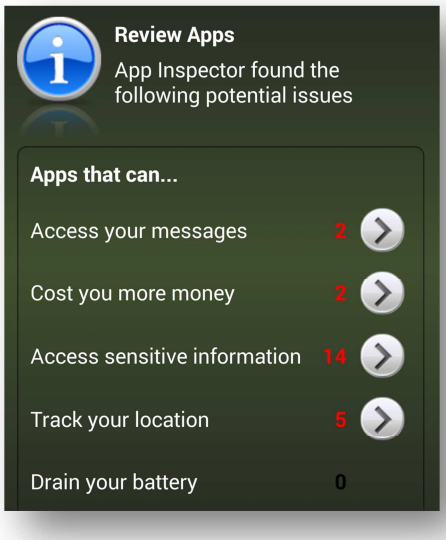
Webroot einen Schutz vor SMS an, die Links zu schadhaften Webseiten enthalten. SMS und Anrufe, die in der Vergangenheit blockiert wurden, sind in einer übersichtlichen Liste aufgeführt. Dort lassen sich nicht nur das Datum, sondern auch der Inhalt der SMS und der Grund des Blocks einsehen.


Detect SMS From Blocked Caller
Detect and notify when an SMS or MMS message is received from numbers contained in your Blocked Numbers list
ON
Block Unidentified Numbers
Block calls where the caller ID is Unknown or Blocked
OFF
Block Malicious SMS
Blocks SMS messages containing links to malicious or phishing websites
ON

In unseren Tests hat das Blockieren von Anrufen wie erwartet geklappt. SMS sind hingegen nicht blockiert worden. Dies führen wir auf Inkompatibilität mit Android 4.4 zurück. Webroot macht auf diesen Zustand jedoch nicht aufmerksam. Auf unserem alternativen Testgerät mit Android 4.1.2 hat auch das Blockieren von SMS funktioniert.

App Inspector

Der App Inspector überprüft installierte Apps auf Risiken, die die Privatsphäre betreffen. Ein Beispiel hierfür wären jene Apps, die auf Nachrichten oder die Ortungsfunktionen Zugriff haben. Durch Antippen einer der Kategorien werden die jeweiligen Applikationen aufgelistet. Für die jeweiligen Apps werden keine weiteren Details angezeigt, es wird lediglich auf den Appmanager von Android weitergeleitet.

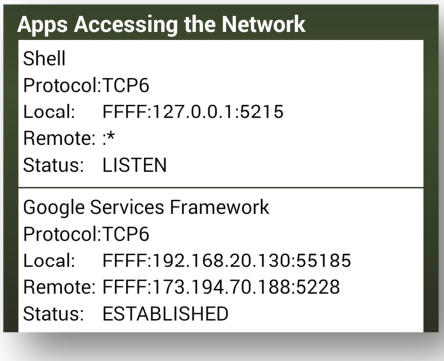

Review Apps
App Inspector found the following potential issues
Apps that can...
Access your messages 2
Cost you more money 2
Access sensitive information 14
Track your location 5
Drain your battery 0

Battery Monitor

Der Batterymonitor gibt detaillierte Informationen zum Akku, wie etwa Ladestatus, die Temperatur und Spannung. Das vom letzten Jahr bekannte Balkendiagramm, welches den Batterieverbrauch der jeweiligen Apps auflistet, konnten wir im diesjährigen Test nicht mehr finden.

Network Monitor

Der Network Monitor listet Details zu Apps auf, die auf das Netzwerk zugreifen. Hierbei wird jeweils der Name des Protokolls, lokale- und remote IP Adressen und Ports, sowie der Status aufgelistet. Durch Antippen eines Eintrags wird eine Whois-Anfrage auf die IP ausführt, und Details wie ISP und ungefährerer Position angezeigt.



Updates

Updates werden automatisch durchgeführt. Hierfür sind die Intervalle stündlich, täglich und wöchentlich einstellbar. Zusätzlich kann ein Update manuell angestoßen werden.

Hilfe

Webroot bietet zu den meisten Funktionen eine umfangreiche Hilfe in Form eines Popups an. Sollte dies dem Nutzer nicht genug sein, so ist zusätzlich eine umfangreiche Hilfedatei verfügbar.

Deinstallation

Für die Deinstallation wird ein Deinstallationsassistent angeboten, der mit einem Klick das gesamte Produkt deinstalliert. Für die Deinstallation ist ein Passwort notwendig, wodurch es einem Dieb nicht möglich ist den Diebstahlschutz zu deinstallieren.

Lizenz

Webroot SecureAnywhere Mobile kann mit einem eingeschränkten Funktionsumfang kostenlos und unbegrenzt verwendet werden. Für anspruchsvollere Nutzer bietet Webroot eine Premiumversion, die zusätzlich einen Deinstallationsschutz, SIM Lock, Wipe und verschiedene App Inspektoren bietet. Diese ist für 3,68€ erhältlich und für ein Jahr gültig.

Fazit

Webroot SecureAnywhere hat sich in unserem Test gut geschlagen. Mit einem verlässlichem Diebstahlschutz und diversen Filtern bietet bereits die kostenlose Version einen guten Schutz. Der Deinstallationsschutz, SIM Lock, und verschiedene App Inspektoren könnten die Premium Version schmackhaft machen. Auch wenn z.B. der Lock vorbildlich gestaltet wurde, sollten Teile des Diebstahlschutzes noch überarbeitet werden.

Fazit

Smartphones sind für einige Personen bereits zum PC-Ersatz geworden. Andere speichern persönliche und berufliche Informationen, die für Kriminelle von großem Interesse sein können. Phishing ist für jeden Gerätetyp mit Zugang zum Internet ein potentieller Angriffspunkt. Durch Hinterlegung der Kreditkartendaten in diversen Shopping Apps, allen voran der Google Play Store, aber auch über den Mobilfunkvertrag können direkt Kosten entstehen – verursacht durch Malware oder einem Unbefugten.

Das Angriffspotential ist groß, vor allem bei einem offenen Betriebssystem wie Android, das den Entwicklern harmloser Apps viele Möglichkeiten bietet was die Programmierung angeht. Bedauerlicher Weise haben Programmierer von Schadsoftware dieselben Voraussetzungen, die oftmals missbraucht werden.

Mobile Sicherheitssoftware schützt den Nutzer vor einem Großteil dieser Gefahren und ist somit unserer Ansicht nach von Smartphones nicht mehr wegzudenken. Trotzdem ist ein großer Teil der Nutzer ohne einer derartigen Schutzeinrichtung unterwegs und einem potentiellen Risiko ausgesetzt. Unverständlich, denn es existieren etliche Produkte, auch kostenlose, die eine große Schutzwirkung mitbringen. Auch das Argument, dass sich Sicherheitsprodukte auf die Performance oder die Batterielaufzeit auswirken, konnten wir in unseren Tests größtenteils widerlegen.

Permissions in Android OS 4.4.2		AhnLab	Avast	Avira	Baidu	Bitdefender	Cheetah C.M.	Cheetah CM S.	Eset	F-Secure	GData	Ikarus	Kaspersky	Kingsoft	McAfee	Qihoo	Quickheal	Sophos	Tencent	TrendMicro	Webroot
Phone calls	directly call phone numbers	•	•	•	•	•		•	•	•	•		•	•	•	•	•	•	•	•	•
	read phone status and identity	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
	reroute outgoing calls		•		•				•	•	•			•	•	•	•		•		
Your messages	edit your text messages (SMS or MMS)	•	•	•	•	•		•	•	•	•		•	•	•	•	•	•	•	•	•
	read your text messages (SMS or MMS)	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•
	receive text messages (SMS)	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•
	receive text messages (MMS)		•						•	•				•	•	•		•	•	•	•
	receive text messages (WAP)							•						•		•			•		
	send SMS messages	•	•	•	•	•		•	•	•	•	•	•		•	•	•	•	•	•	•
Camera	take pictures and videos		•	•	•		•	•	•			•	•	•	•	•	•		•		
Microphone	record audio		•		•											•	•				
Your location	approximate location (network-based)		•	•	•	•		•		•	•				•	•	•	•	•		•
	precise location (GPS and network-based)	•	•	•	•	•		•	•	•	•	•	•		•	•	•	•	•	•	•
Your social information	modify your contacts	•	•	•	•	•		•	•	•	•		•		•	•	•	•	•	•	•
	read call log	•	•	•	•	•		•	•	•	•		•	•	•	•	•	•	•	•	•
	read your contacts	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•
	write call log	•	•	•	•	•		•	•	•	•		•	•	•	•	•	•	•	•	•
Your personal information	activity recognition								•												
	add or modify calendar events and send email to guests without owners´ knowledge	•	•						•				•				•			•	•
	read calendar events plus confidential information	•	•						•				•				•			•	•
	modify your own contact card								•												
	read your own contact card								•	•											
Bookmarks and History	write web bookmarks and history	•	•	•		•	•	•	•	•		•	•		•	•	•	•	•	•	•
	read your Web bookmarks and history		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Storage	modify or delete the contents of your USB storage	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
	read the contents of your USB storage	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Alarm	set an alarm						•														
Lock screen	disable your screen lock		•	•					•			•			•				•		
Your accounts	add or remove accounts	•		•		•		•	•	•	•		•				•			•	•
	find accounts on the device		•	•	•	•	•	•	•	•	•	•	•		•	•	•			•	•
	read Google service configuration		•	•		•		•			•										
	use accounts on the device		•			•		•		•	•				•						•
	create accounts and set passwords	•									•										•
Read user dictionary	read terms you added to the dictionary		•																		
Network communication	change network connectivity	•	•		•	•	•		•				•	•		•	•		•		
	connect and disconnect from Wi-Fi	•	•		•	•	•		•	•	•		•	•	•	•	•		•	•	
	control Near Field Communication									•							•	•			
	Google Play billing service		•			•			•	•	•	•	•		•		•			•	•
	Google Play license check		•							•	•	•			•		•				
	receive data from Internet		•	•		•	•	•	•	•	•		•		•		•			•	•
	full network access	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
	view network connections	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
	view Wi-Fi connections	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•
Bluetooth	access Bluetooth settings				•					•			•	•	•	•			•		
	pair with Bluetooth devices				•	•				•			•	•	•	•			•		
Your application information	close other apps	•	•		•		•			•			•	•	•	•	•	•	•	•	•
	reorder running apps										•				•		•				
	retrieve running apps	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
	run at startup	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•
Other Application UI	draw over other apps		•	•	•	•	•	•	•	•		•		•	•	•	•		•	•	•
Affects Battery	allow Wi-Fi Multicast reception				•										•						
	control flashlight				•														•		
	control vibration		•		•	•	•			•			•	•	•	•	•		•	•	
	prevent phone from sleeping		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Wallpaper	adjust your wallpaper size				•																
	set wallpaper				•					•											
Write user dictionary	add words to user-defined dictionary		•																		
Audio Settings	change your audio settings			•	•	•		•					•		•	•	•			•	
Sync Settings	read sync settings				•					•	•		•			•	•				
	read sync statistics				•																
	toggle sync on and off				•					•	•		•		•	•	•		•		•
Status Bar	expand/collapse status bar				•		•						•	•			•				
System tools	access extra location provider commands					•							•						•		
	delete all app cache data				•		•		•						•	•			•		
	install shortcuts				•		•	•		•				•		•	•		•		
	measure app storage space		•		•		•				•			•	•	•			•	•	•
	mock location provider commands												•								
	mock location sources for testing												•							•	
	modify system settings	•	•		•	•	•			•	•		•	•	•	•	•		•		
	read Home settings and shortcuts						•														
	read subscribed feeds												•								
	send sticky broadcast		•		•		•				•			•					•		
	uninstall shortcuts				•		•									•	•		•		
	write Home settings and shortcuts						•														

Feature List Android Mobile Security (as of August 2014)	FREE	COMMERCIAL	FREE	FREE	COMMERCIAL	FREE	FREE	COMMERCIAL	COMMERCIAL	COMMERCIAL	COMMERCIAL	COMMERCIAL	FREE	FREE	FREE	COMMERCIAL	FREE	FREE	FREE	COMMERCIAL	COMMERCIAL
Product Name	AhnLab V3 Mobile Plus	avast! Mobile Security	Avira Antivirus Security	Baidu Mobile Security	Bitdefender Mobile Security	CheetahMobile Clean Master	CheetahMobile CM Security	ESET Mobile Security	F-Secure Mobile Security	G Data Internet Security for Android	IKARUS mobile.security	Kaspersky Internet Security	Kingsoft Mobile Security	McAfee Mobile Security	Qihoo 360 Mobile Security	Quick Heal Total Security	Sophos Mobile Security	Tencent Mobile Security Manager	Trend Micro Mobile Security	Webroot SecureAnywhere Mobile Complete
Version Number	2.1	3.0.7751	3.5	5.2.0	2.23.423	5.6.0.1600	1.6.1.1632	3.0	9.2	25.4.0	1.7.21	11.5.4.704	3.3.1.1503	4.2.0.527	2.1.0	2.0.022	3.5.1324	4.8	5.0.0.1247	3.6.0.6610
Supported Android versions	2.2 and higher	2.2 and higher	2.2 and higher	2.2 and higher	2.3.3 and higher	2.2 and higher	2.2 and higher	2.3 and higher	2.3.3 and higher	2.1 and higher	2.2 and higher	2.3 and higher	2.2 and higher	2.3 and higher	2.2 and higher	2.3 and higher	2.3.3 and higher	2.1 and higher	2.3 and higher	2.2 and higher
Supported Program languages	English, Korean	English, Czech, French, Italian, Spanish, German, Russian, Portuguese, Catalan, Hungarian, Dutch, Polish, Turkish, Vietnamese, Chinese, Japanese, Bulgarian	English, German, French, Italian, Spanish, Korean, Japanese, Portuguese	Chinese	English, Portuguese, French, German, Italian, Polish, Romanian, Spanish, Turkish, Vietnamese	Chinese	English, Russian, Spanish, Italian, Indonesian, Turkish, German, Portuguese, French, Vietnamese, Arabic, Thai, Japanese, Korean, Hungary, Croatian, Greek, Malay, Dutch, Slovak, Bulgarian, Ukrainian, Polish, Serbian, Chinese	English, Polish, Danish, Finnish, Norwegian, Japanese, Russian, Hungarian, Spanish, German, Portuguese, Dutch, French, Romanian, Turkish, Swedish, Chinese, Italian, French, Korean, Czech, Hebrew, Slovak, Vietnamese, Arabic, Bulgarian, Thai	English, Bulgarian, Chinese, Croatian, Czech, Danish, Dutch, Finnish, French, German, Greek, Hungarian, Indonesian, Italian, Japanese, Korean, Malay, Norwegian, Polish, Portuguese, Romanian, Russian, Spanish, Swedish, Tagalog, Thai, Turkish	German, English, French, Spanish, Portuguese, Italian, Dutch, Polish, Russian, Turkish, Japanese, Chinese	English, German, Italian, French, Spanish, Russian, Chinese, Turkish	English, Russian, German, French, Spanish, Italian, Portuguese	Arabic, Bulgarian, Czech, Danish, German, Greek, English, Spanish, French, Hebrew, Hindi, Croatian, Hungarian, Indonesian, Italian, Japanese, Korean, Malay, Norwegian, Dutch, Polish, Portuguese, Romanian, Russian, Slovak, Serbian, Thai, Turkish, Ukrainian, Vietnamese, Chinese	English, Danish, German, Greek, Spanish, Finnish, French, Indonesian, Italian, Japanese, Korean, Norwegian, Dutch, Portuguese, Russian, Swedish, Turkish, Chinese	English, Chinese	Japanese, Korean, Italian, Spanish, French, German	English, German, French, Italian, Japanese, Chinese	Chinese	English, German, Spanish, French, Italian, Korean, Dutch, Portuguese, Chinese, Turkish, Vietnamese	English, Japanese, Chinese, Dutch, German, French, Italian, Korean, Portuguese, Spanish, Turkish, Russian
Anti-Malware																				
On-Install and On-Demand scan of installed apps	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
On-Demand scan (File system)	●	●	●	●		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
On-Access scan for files		●				●		●	●	●	●	●				●	●	●		●
Scan works offline	●	●	●	●		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Scan is assisted by cloud		●	●		●	●	●	●	●	●		●	●	●	●		●	●	●	●
Automatic (scheduled) Scan	●	●					●	●	●	●	●	●		●		●	●	●	●	●
Safe Browsing (Anti-Phishing & Anti-Malware)		●			●	●	●	●	●	●	●	●	●	●	only on rooted phones	●	●	●	●	●
Scan installed apps for (possible) privacy violations		●		●	●		●	●	●	●			●	●	●	●	●	●	●	●
Quarantine							●	●				●				●	●			●
Recommendations for android settings				●				●						●		●	●	●		●
USSD Blocking		●	●					●		●	●	●	●	●			●			●
Anti-Theft																				
Remote Lock & Remote Wipe	●	●	●		●		●	●	●	●	●	●		●		●	●	●	●	●
Remote Locate	●	●	●		●		●	●	●	●	●	●		●		●	●	●	●	●
Continous Locate (Track the movement of the phone)		●						●						●		●				
Remote Alarm		●	●		●		●	●	●	●	●	●		●		●	●	●	●	●
Remote Unlock		●	●				●	●	●					●		●	●	●		
SMS commands for controlling Anti-Theft features	●	●			●		●	●	●	●	●	●		●		●	●	●		●
Webinterface for controlling Anti-Theft features		●	●		●		●	●				●		●		●		●	●	●
Lock on SIM Change	●	●					●	●	●	●	●	●		●		●		●	●	●
Notify on SIM Change (Email / SMS)	●	●			●		●	●	●	●		●		●		●	●	●		
Anti Spam																				
Whitelist / Blacklist SMS	●	●	●	●				●	●	●	●	●	●	●	only on rooted phones	●	●	●	●	●
Whitelist / Blacklist Phonecalls	●	●	●	●			●	●	●	●		●	●	●		●	●	●	●	●
Whitelist / Blacklist with wildcards		●		●				●		●		●	●	●		●	●	●		
Blocking of SMS containing keywords	●			●								●		●		●		●	●	●
Parental Control																				
Safe Webbrowsing		●			●		●		●	●	●		●	●		●	●		●	●
Lock Apps		●			●		●		●	●				●			●	●		
App launcher especially for kids (Parents can choose apps)										●				●						
Authentication																				
Uninstallation protection (password required for uninstallation)		●			●			●	●	●	●	●		●		●	●	●	●	●
Settings protected with password		●						●	●	●	●	●				●	●	●	●	
User Account needed to use product			●		●					●		●							●	●
Additional features																				
Backup		●								●				●		●		●	●	
Network monitor	●	●		●				●						●		●		●		●
Local Wipe		●		●	●							●		●		●				
Task Killer		●		●		●							●			●		●		
Battery Monitor								●					●							●
Support																				
Email support	●	●	●		●	●	●	●	●	●	●	●	●	●	●	●		●	●	●
Online Help	●	●	●		●	●	●	●	●	●		●	●	●	●	●	●	●	●	●
FAQ		●	●	●	●	●	●	●	●	●		●	●	●	●	●	●	●	●	●
User Forum		●	●		●	●	●	●	●			●	●	●	●	●	●	●	●	●
User Manual	●	●	●	●	●			●	●	●	●	●		●	●	●		●		●
Phone Support		●	●		●	●		●	●	●	●	●		●	●	●		●	●	●
Online Chat					●	●						●	●	●	●	●		●		
Supported languages of support	English, Korean	English, Czech, French, Spanish, Portuguese, Turkish, Polish, Russian, German, Chinese, Italian	German, English, French, Italian, Dutch, Russian, Spanish, Portuguese, Chinese, Japanese, Malaysian, Korean	Chinese	English, French, Italian, Spanish, Portuguese, Romanian, German, Turkish	Chinese	Chinese	All	English, German	German, English, Spanish, Italian, French, Portugese, Chinese, Japanese	English, German	English, Russian, German, French, Spanish, Italian, Portuguese	Chinese	Spanish, English, Portuguese, Czech, Danish, German, French, Chinese, Italian, Japanese, Dutch, NOrwegian, Polish, Russian, Suomi, Swedish, Turkish, Korean	Chinese	Hindi, English, Japanese	English, German, French, Italian, Japanese, Chinese	Chinese	English	All

Copyright and Disclaimer

This publication is Copyright © 2014 by AV-Comparatives®. Any use of the results, etc. in whole or in part, is ONLY permitted after the explicit written agreement of the management board of AV-Comparatives, prior to any publication. AV-Comparatives and its testers cannot be held liable for any damage or loss which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but a liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data.

For more information about AV-Comparatives and the testing methodologies please visit our website.

AV-Comparatives (September 2014)